Between Effort and Security: User Assessment of the Adequacy of Security Mechanisms for App Categories

Christian Reuter
Science and Technology for Peace and Security (PEASEC), Technische Universität Darmstadt

Katja Häusser
Science and Technology for Peace and Security (PEASEC), Technische Universität Darmstadt

Mona Bien
Science and Technology for Peace and Security (PEASEC), Technische Universität Darmstadt

Franziska Herbert
Science and Technology for Peace and Security (PEASEC), Technische Universität Darmstadt

ABSTRACT

With the increasing popularity of the smartphone, the number of people using it for financial transactions such as online shopping, online banking or mobile payment is also growing. Apps used in these contexts store sensitive and valuable data, creating a need for security measures. It has not yet been researched to what extent certain authentication mechanisms, which can be information-, biometric- as well as token-based, are suitable for individual apps and the respective data. The goal of this work is to assess how perceived security and estimated effort of using such mechanisms, as well as the degree to which app data is considered worth protecting, influence users' choices of appropriate measures to protect app categories. Therefore, we conducted a representative study (n=1024). On the one hand, our results show that a positive correlation between perceived security and effort exists for all investigated non-biometric authentication methods. On the other hand, the study sheds light on the differences between the investigated app categories and the users' choice of the appropriate security mechanisms for the particular category. In contrast to perceived security having a positive influence on a user's preference of mechanism, a relation can hardly be identified for effort. Moreover, app data sensitivity does not seem relevant for the users' choice of security mechanism.

CCS CONCEPTS

• **Human-centered computing → Smartphones** • Human-centered computing → Empirical studies in collaborative and social computing Human-centered Computing

KEYWORDS

Security, Usability, Usable Security, Apps, Smartphone Security, Security Mechanisms, Effort, User Assessment

ACM Reference Format:

Christian Reuter, Katja Häusser, Mona Bien and Franziska Herbert. 2019. Between Effort and Security: User Assessment of the Adequacy of Security Mechanisms for App Categories. In *Mensch und Computer 2019 (MuC'19), September 8—11, 2019, Hamburg, Germany*. ACM, New York, NY, USA. 11 pages. https://doi.org/10.1145/3340764.3340770

MuC '19, September 8—11, 2019, Hamburg, Germany

ACM ISBN 978-1-4503-7198-8/19/09...$15.00
https://doi.org/10.1145/3340764.3340770

1 Introduction

54 million German citizens are using a smartphone nowadays [31]. This corresponds to 78% of the population, more than twice as many as in 2012. Especially in the younger age groups, more than 90 % own a smartphone. The vast majority of Germans can no longer imagine a life without it. There is a good reason for this, as the smartphone is used in different fields of life: Apart from phone calls, users benefit from camera, social contact, search engine, banking and shopping features [31]. Particularly, the usage of apps in the field of banking and shopping has shown a positive trend: While studies conducted in 2012 showed that the laptop was preferred as the most secure method for financial transactions on mobile devices [10, 33], in 2016, the number of those using their smartphone to buy products almost doubled [1]. Similar trends can be observed for mobile payments, i.e., payment processing via smartphone/tablet. While users in 2012 were skeptical, in 2015, already 25% of Germans were using it, and further 35% indicated their intention to try it in the future [38].

It is hardly surprising that the growing use of apps is related to the fact that confidential and valuable information is increasingly stored on the smartphone. In case of smartphone loss or theft, this may cause serious harm for the user, as accounts and data could be abused. That is why 56% of Germans would rather leave their house unlocked for one day than their smartphone unlocked on a park bench for one hour [12]. It is not only the screen lock that protects data on the smartphone. There are several apps having security mechanisms that require authentication, e.g., by password, fingerprint or TAN procedure. However, are they appropriate for the respective app, considering their security and the effort to use them?

The interface between IT security and usability is often summarized under the term "usable security", which focuses on the user-friendly design of security mechanisms [36, 40]. Studies in the field of smartphones mostly concentrate on individual protection, e.g. [37, 42], primarily on functions as screen lock, e.g. [2, 4, 9, 15, 19, 34, 41]. Up to now, there is no focus on authentication mechanisms for individual apps, and the sensitivity of data stored on the smartphone has not yet been considered extensively. Harbach et al. [19] found that sensitive data was mostly only secured through screen lock and suggest to secure sensitive data specifically instead of using an overall screen lock. Therefore, the central question discussed in this study is:

Which security mechanisms, in view of perceived security, effort and need for protection of data, do smartphone users consider to be appropriate for different app categories? To investigate this question, hypotheses were formulated based on related work and verified in the context of a representative survey. The results are analyzed and discussed.

2 Current State of Research

The topic of smartphone security is a widespread field of research. Given the object of research, mainly three aspects are considered: Authentication mechanisms regarding their security, usability, and user preferences, sensitive data considered worthy of protection on mobile devices, and the users' motivation to (not) use security mechanisms.

Many studies on smartphone security already exist. Usage, security, and usability of various authentication mechanisms are examined e.g. [2, 41, 43, 48]. However, the mechanisms are viewed almost exclusively as a screen lock to protect all smartphone data e.g. [4, 9, 15, 19, 34]. A differentiated investigation of the users' assessment of security and effort of authentication methods used to protect individual app categories has not yet been undertaken. Additionally, stored data show different levels of sensitivity depending on the app or field of application [2, 17]. However, most studies on the degree to which data are worth protecting differentiate based on data types [10, 33, 34] and not on app categories. Studies on users' assessment mainly focus on reasons for the (non-)usage of authentication mechanisms [3, 9, 15, 19, 22, 35, 41, 46] and not on the users' assessment of the adequacy of these mechanisms for different purposes. Harbach et al. [19] found, that in 24 % of their smartphone usage users considered unlock screens unnecessary. They also found that users access sensitive data in only around 25 % of their smartphone usage time. They therefore suggest to specifically secure sensitive data instead of using a screen lock. Micallef et al. [30] designed a context-sensitive screen locking application, which was evaluated positively by participants: They rated it efficiently, reasonable secure and not annoying. This indicates the need for an investigation of app specific authentication mechanisms. Concerning users' choices of authentication mechanisms, numerous studies have already shown that assessments of authentication mechanisms differ among users [2, 4, 6, 9, 26, 41, 45]. Gerber and Zimmermann [17] identified two different user groups, one preferring text passwords and one preferring biometric authentication but for the same reasons: efficiency, security and habit. Ben-Asher et al.[2]also reported that perceived security and effort must be balanced to achieve an appropriate security behavior of users. They [2] also reported that the sensitivity of the data has significant implications for the use of authentication mechanisms. However, the degree to which smartphone data is worth protecting has only been assessed in general or with regard to different types of data so far [33, 34]. Concerning the users' choice of authentication mechanism, is has also to be noted that users also evaluate different security mechanisms differently concerning their security as well as concerning the effort of using them, which was shown by e.g. [3, 5, 22, 27, 29, 34]. In summary, it can be stated that in previous studies on smartphone security, users assessed security mechanisms according to security and effort [2, 4, 6, 9, 19, 26, 41], and smartphone data were investigated with regard to the degree to which it is considered worthy of protection [2, 33, 34]. In all cases, the users' rating was examined. However, there is a lack of knowledge regarding the potential influence of perceived security of security mechanisms, estimated effort to use them, the users` assessment of data worth protecting, and the interaction between these factors on the use of security for a diverse set of app categories.

3 Method

In order to address the central question of this study, a questionnaire was administered. This methods seems suitable, as many related studies also use questionnaires, e.g. [17, 19, 30]. Additionally, an online survey allows the sampling of a large number of people in limited time [23].

3.1 Research Goal and Study Design

Meanwhile, more and more apps that may contain sensitive data have protective mechanisms. These are either obligatory because of regulatory conditions, as in mobile banking, or available as an optional function and range from password to fingerprint up to TAN procedures. However, currently, it is not clear whether these security mechanisms are considered appropriate by the users. Therefore, the purpose of this study is to answer this question regarding the mechanisms' perceived security and effort as well as the estimated data sensitivity in various app categories. For this purpose, three research questions (RQ) were formulated, from which hypotheses (H) were subsequently derived. To test these hypotheses, several questions (Q) were developed for the study.

3.1.1 RQ1: How do users rate different security mechanisms for apps in terms of security and effort?

The purpose of this research question is to identify how users assess the security and effort of various security mechanisms used to protect app data. Using the results, security and effort can be investigated as potential factors influencing the choice of adequate security mechanisms for the protection of different app categories (RQ3). Three hypotheses can be formulated to investigate the research question:

H1.1: **Users evaluate different security mechanisms differently with respect to security** Numerous studies have confirmed this [2, 4, 34, 41].These results are expected to be replicated for selected security mechanisms.

H1.2: **Users evaluate different security mechanisms differently with respect to the effort of using**. Previous research has shown that the evaluation of usability or effort of different security mechanisms varies [2, 32, 34, 41]. The results are now expected to be replicated in terms of the subjective effort of selected security mechanisms.

H1.3**: Security mechanisms credited with higher security are perceived as more complex to handle**. In the literature, the tension between security and effort is discussed, since higher security usually entails extra work. Concepts for reducing stress are proposed [8, 20, 21, 28, 30]. The hypothesis examines whether a correlation between perceived security and effort is also present for the considered security mechanisms.

To test these hypotheses, the following questions were formulated: Q1: **To unlock a smartphone and to log into individual apps, various security mechanisms are used. Please assess the security measures that you know according to the degree of security you attribute to them.** To formulate this question, security mechanisms had to be selected for evaluation. The users evaluated the mechanisms on a five-point scale from *very secure* to *not secure at all*. In addition, they could also select the answer *I do not know*. With this question, H1.1 can be verified directly. Q2: **The use of a security mechanism to unlock a smartphone or to log into an app always involves a certain effort for the user. Please assess the security mechanisms that you know according to the degree of effort you attribute to them.** The security mechanisms were rated on a five-point scale from *very complex* to *not complex at a*ll. Apart from this, participants had the option *I do not know*. With this question, H1.2 can be verified directly. To test H1.3, the results of Q1 and Q2 must be considered simultaneously.

3.1.2 RQ2: How do users rate different app categories regarding the degree to which the data contained is worth protecting?

Studies confirm that data which requires protection is stored on the smartphone [2, 10, 32, 34]. This research question intends to examine the need for protection of data in different app categories. Using the results, we can verify whether protection is an influencing factor for the choice of an appropriate security mechanism for the respective app category (RQ3).

To investigate the research question, the following hypothesis can be formulated: H2: **The users assess the data contained in different app categories differently regarding its need for protection (sensitive and/or valuable)**. Data worth protecting may be sensitive and/or valuable [33]. The hypothesis is formulated to show how the degree to which data is seen as worth protecting varies with respect to different app categories.

To test the hypothesis, the following question was formulated: Q3: **Apps on mobile devices also store personal information of the user. Please assess to what extent your data in the different app categories you are using is worth protecting. To evaluate this, consider how sensible and valuable the data is for you in case of loss.** To assess the degree to which data is worth protecting, relevant app categories had to be determined. The app category was evaluated on a five-point scale from *very protection-worthy* to *not protection-worthy at all*. Additionally, the option *I do not use* was available.

3.1.3 RQ3: What security mechanisms do users consider appropriate for different app categories in terms of security, effort, and degree to which data is worth protecting?

Relationships between security, effort, and need for protection of data have already been shown: Ben-Asher et al. [2] found that the effort invested in protecting data correlates with the sensitivity of the data when using authentication procedures. In terms of solutions, Melicher et al. [29] suggested passwords with variable levels of effort, depending on data sensitivity. Dörflinger et al. [14], in turn, presented a concept in which secure authentication mechanisms are used for sensitive data and less secure ones are used for insensitive data. First, it should be determined which security mechanisms users consider suitable for different app categories. Subsequently, the influence of perceived security, effort, and the need for protection of the app data on the choice of the mechanism for the protection of the app category will be examined.

To investigate the research question, three hypotheses can be formulated:

H3.1: **Users consider different security mechanisms appropriate for different app categories.** Gerber and Zimmermann [17] showed that depending on the application context, on the laptop, different security mechanisms are considered adequate. This hypothesis tests the assessment of app categories on the smartphone.

H3.2: **For app categories with more sensitive data, users choose security mechanisms which they perceive to be more secure.** Dörflinger et al. [14] suggested a concept reflecting this relation. To examine whether users act accordingly, the influence of security on the selection frequency of the security mechanism is determined. Subsequently, the relation to the need for protection of the data is examined.

H3.3**: Users accept security mechanisms with higher effort in the context of app categories with data worth protecting**. Ben-Asher et al. [2] proved a correlation between the sensitivity of the data and tolerated effort, while Melicher et al. [29] introduced the concept of usable security on the basis of this principle. The hypothesis will test whether the relation is also valid for the examined authentication methods and app categories. In the first step, the influence of perceived effort on the frequency of selection of the respective mechanism is analyzed. Subsequently, the subjective data sensitivity is included in the analysis.

To investigate the hypotheses, the following question is formulated: Q4**: In the context of the app categories which you are using yourself, please evaluate which security mechanisms you consider appropriate for the protection of your data. You can select one or more security mechanisms per app category.** In addition to the mentioned authentication measures, the options per app category included *smartphone lock* (if the screen lock is considered sufficient to protect the app data), *none* (if the app category does not require protection) and *I do not use it.* H3.1 can be verified using this question. For H3.2, the results of Q1, Q3 and Q4 must be considered jointly, and for investigating H3.3, it is necessary to combine the results of Q2, Q3, and Q4.

The four questions on security (Q1), effort (Q2), need for protection (Q3), and appropriateness (Q4) were placed at the end of a questionnaire on social media in crisis situations and examined in a survey. In addition to the results of the four questions, the demographic data of the participants on gender, age, educational level, net household income, federal state, and their use of smartphones is interesting since this could have influenced the answer.

3.2 Security Mechanism and App Categories

To formulate the concrete questions for the survey, security mechanisms had to be selected that are typically used to protect app data. In addition, it was necessary to determine app categories containing potentially sensitive data. The following section illustrates how this selection was made, and which mechanisms and categories were examined in the study.

Two forms of app locks can be observed in **security mechanisms**: on the one hand, smartphone settings and security apps make it possible to set up barriers for specific apps, and on the other hand, many apps have their own authentication methods. App locks set up via smartphone settings usually utilize the mechanisms that can also be used for the screen lock, such as PIN, pattern or fingerprint. [42] analyzed different authentication mechanisms like token-based authentication, slide lock and biometric authentication and found that every mechanism has positive and negative aspects concerning security and usability. A PIN for example is easy to remember for the user but weak with regards to security whereas fingerprint as authentication is more secure and also user-friendly but expansive[42]. With their work Shafique et al.[42]provide a comparative analysis of different authentication mechanisms, also with regards to their security. As this work focuses on app authentication mechanisms, only app-specific authentication mechanisms were searched for and about 30 popular apps were considered. Our analysis showed that for authentication, it is often required to log in to the user account by e-mail and password (e.g., Amazon, Facebook, Dropbox). For some apps, app-specific passwords or PINs can be generated and used for authentication purposes (e.g., Sparkasse, German banking institution). In addition, some apps offer the possibility to authenticate with a fingerprint (e.g., GMX Mail). To first log in, TAN procedures are used in some cases. For example, in the app of the Techniker Krankenkasse (German health insurance provider), a TAN is sent to the user via mail, while in the messenger app Telegram, the TAN is sent to another terminal on which the application is installed. TAN procedures are also used for authentication in transactions in mobile banking apps (e.g., Sparkasse). In a pilot project, MasterCard checks the usage of fingerprints and face scan instead of TANs for authentication during transactions [13]. Also, Santander's SmartBank banking app makes it possible to perform various actions per voice command during *voice banking* [16]. Another security mechanisms, implicit authentication, was rated as more convenient as explicit authentication by users [26] but was not investigated in this study as none of the mentioned apps used it. Based on the results of the research, eight security mechanisms were selected for examination in this study**: password, e-mail & password, PIN, pattern (information-based), fingerprint, face recognition, voice recognition (biometric), TAN procedure (token-based).**

In addition to the security mechanisms, **app categories** had to be selected whose data could be evaluated for sensitivity, and for which appropriate mechanisms could be indicated by users. Our categories are based on application fields of the smartphone derived from a study by Bitkom [31]. Two categories with similar data have been grouped together: health and fitness as well as mobile shopping and ticketing. Remote control and networking applications have been combined under remote control. Cloud services have also been added as an app category with potentially sensitive data. This results in nine app categories for investigation in this study: **social networks, short messaging service, e-mail, mobile banking, health/fitness, mobile shopping/ticketing, remote control, dating, cloud services.**

3.3 Participants and Analysis

The presented questions are taken from a representative online survey, which we conducted in Germany in July 2017, using the ISO-certified panel provider GapFish (Berlin). GapFish guarantees panel quality, data quality, and security, as well as survey quality through various (segmentation) measurements for each survey within their panel of 180,000 active participants. Our overall survey included 30 questions in total and also covered other topics, such as [18, 24, 25, 39]. In this work, we examine the four questions mentioned in section 3.1 (Questions 27 – 30 in the survey). The respondent sample (n=1024) was adapted to the distribution of age, region, education, and income according to the general German population [5, 7, 44]. Participants were solely recruited by GapFish based on the before mentioned criteria, e.g. age and region.

For the analysis, we used Microsoft Excel with the statistical add-in XLSTAT [47]. The results of the survey were numerically coded. Subsequently the answer options *I do not know* and *I do not use* were removed from the data and excluded from the analysis as missing values. For all questions, the frequencies were considered first. A Shapiro-Wilk test showed deviations from a normal distribution for the variables security, effort and need for protection ($p < 0.0001$). Thus, a non-parametric Kruskal-Wallis test was used for the analysis. To test the relationships between the variables security, effort, need for protection and the frequency of selection (H1.3, H3.2, H3.3), the Spearman rank correlation was used. The influence of gender, age, educational level, net household income, state, and smartphone usage on the assessments of security, effort and need for protection was examined by means of chi-square tests in contingency tables. In this context, the values were aggregated across all security mechanisms and app categories. Correlations between the demographic variables were not considered.

4 Results I: Security Mechanisms- Security and Effort

Concerning RQ1, the survey provided the following results:

H1.1: Users evaluate different security mechanisms differently with respect to security. In Q1, the participants assessed various authentication mechanisms according to their security. The results are shown in Figure 1. The fingerprint was most frequently chosen as a secure mechanism (79%, *very secure* + *fairly secure*), closely followed by face recognition (72%). E-mail & password (62%), PIN (61%), TAN (60%) and password (59%) received almost identical results and were slightly ahead of voice recognition (53%). The pattern is viewed to be the least secure (30%). The Kruskal-Wallis test (H (7) = 692.83, p < 0.0001) proved the statistical significance of differences in the assessments of the security mechanism and thus confirmed H1.1.

The chi-square test has shown that the distribution of the answers, including the gender of the participants, is significantly different from a theoretical equal distribution. Women less often tend to rate the mechanisms as *not secure at all* / *hardly secure*. Also, in terms of age, educational level, net household income, federal state of origin, and smartphone usage, significant differences were found. Older participants chose *very secure* less often than expected. Participants with a lower educational level and net household income rated the mechanisms as more secure than those with higher education and those with higher household incomes. There were no trends for the federal state and smartphone usage. The statistical results of the chi-square test can be found in table 6 in the appendix.

H1.2: Users evaluate different security mechanisms differently with respect to the effort of using. In Q2, participants were asked to assess security mechanisms regarding the respective anticipated effort. The results are displayed in Figure 2. Participants viewed the combination of e-mail & password as the most complex security mechanism (35%, *very complex* + *fairly complex*), followed by TAN method (30%) and password (28%). Face and voice recognition were rated equally (21%), closely followed by pattern (18%), fingerprint (17%) and PIN (17%). Least effort was attributed to the fingerprint (65%, *not complex at all* + *hardly complex*), closely followed by PIN (60%), pattern (59%), face (58%) and voice recognition (56%) and distantly followed by password (47%), TAN procedures (38%) and e-mail & password (37%). The Kruskal-Wallis test showed statistical significance of differences in the assessments (H (7) = 371.27, p < 0.0001) and thus confirmed H1.2.

With regard to potential factors influencing the assessment of the effort of the mechanisms, the chi-square test revealed significant differences to the theoretical equal distribution for the variables gender, age, educational level, net household income, federal state of origin, and smartphone usage. Men rated the security mechanisms significantly more often as *very/fairly complex* than women, who often chose *moderately/hardly complex*. Younger age groups as well as participants with lower net household incomes tend to consider the mechanisms more complex than older ones and participants with higher net household incomes. By contrast, there was no clear trend for educational level, federal state and smartphone use. The statistical results of the chi-square test can be found in table 7 in the appendix.

H1.3: Security mechanisms with higher security are perceived as more complex. The Spearman correlation was used to examine whether a relation exists between the assessments of security and effort. There were significant correlations for the password, e-mail & password, PIN, pattern and TAN procedure, but not for fingerprint, face and voice recognition (see Table 1). All significant correlations are positive, which means that a higher level of security is associated with a higher level of effort. The effect size can be described as low (r = 0.1) for TAN procedure, PIN, e-mail & password as well as password, and for the pattern as medium (r = 0.3). The results partially confirm H1.3, only biometric security mechanisms are excluded from the correlation.

Security mechanism	Password	E-Mail & password	PIN	Pattern	Fingerprint	Face recognition	Voice Recognition	Tan procedure
Amount	1013	1006	1013	928	1006	983	986	986
Correlation coefficient r Security – Effort	0.204	0.155	0.130	0.316	-0.032	-0.023	0.048	0.105
P value	<0.0001	<0.0001	<0.0001	<0.0001	0.323	0.481	0.145	<0.0001

Table 1. Results of the Spearman correlation for security and effort.

5 Results II: App Categories- Data Worth Protecting

With regard to RQ2, the survey provided the following results:

H2: The users assess the data contained in different app categories differently regarding its need for protection (sensitive and/or valuable). In Q3, the participants were asked to assess the need for protecting data in app categories of which they themselves use apps. The results are displayed in Figure 3. Mobile banking is regarded as most worthy of protection (88% *very protection-worthy* + *fairly protection-worthy*). The second most sensitive category is e-mail (73%), followed by remote control (62%), short messaging services (61%), cloud services (58%), and mobile shopping/ticketing (58 %). The categories social networks (52%) and health/fitness (44%) are rated as less sensitive. Dating (36%) is least protection-worthy. Dating is least popular among the app categories (31% *I do not use*), followed by cloud services (23%) and remote control (22%). With only 2% non-users, e-mail is the most commonly used app category. The Kruskal-Wallis test (H (8) = 970.68, p < 0.0001) showed statistical significance of differences in the need for protection and thus confirmed H2.

Examining potential influential factors on the assessment of need for protection, significant differences could be found in the chi-square test for the variables age, educational level, net household income, federal state of origin, and smartphone usage. For the gender variable, there was no significant difference to the theoretical equal distribution of responses. The statistical results of the chi-square test can be found in table 8 in the appendix. Regardless of the chi-square test, it was noticeable that with increasing age, some app categories were less frequently used. There are also differences in smartphone usage regarding the use of app categories: Participants who use their smartphone more frequently also tend to use more app categories. Apart from the usage frequency, few correlations between the variables and the assessment of the need for protection could be established. Only with respect to net household income, it could be observed that participants with lower incomes rate app categories less often as worthy of protection.

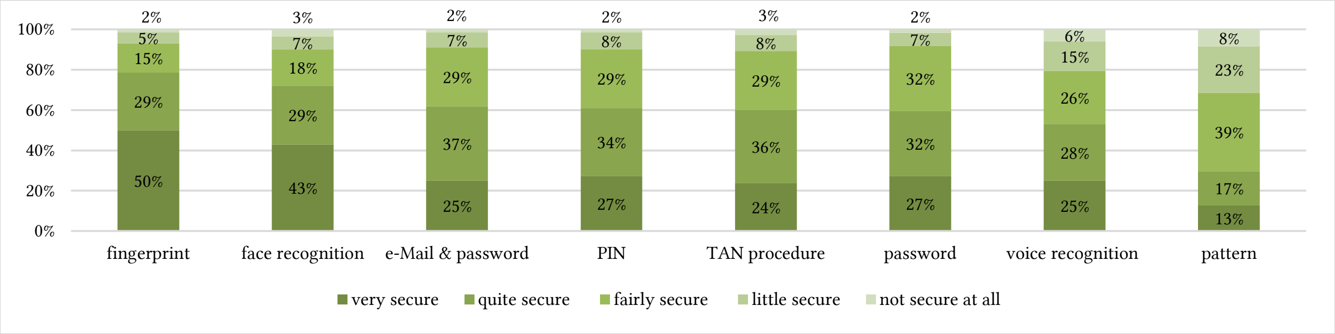


Figure 1. Assessment of the security of the investigated authentication mechanisms.

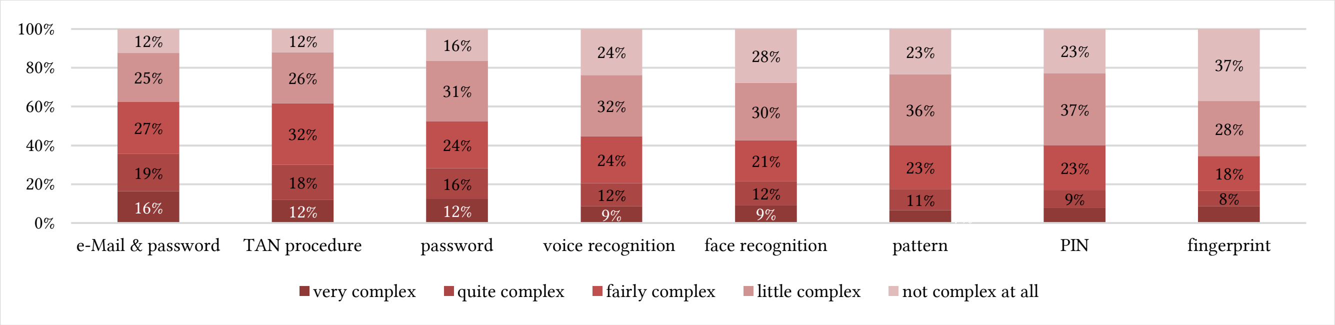


Figure 2. Assessment of the effort of the investigated security mechanisms.

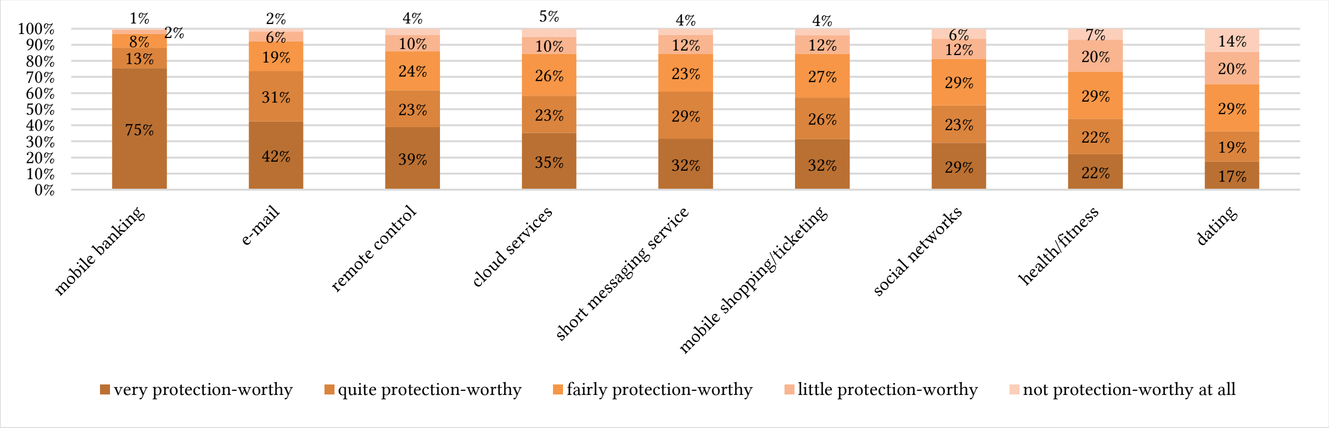
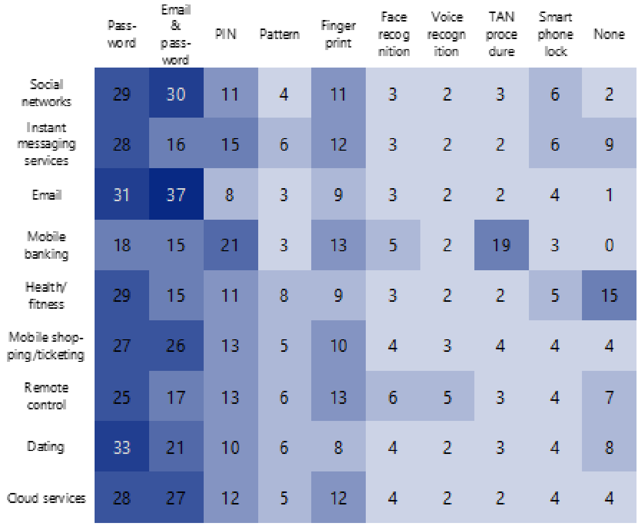


Figure 3. Assessment of the need for protection of the data in the examined app categories.

6 Results III: Appropriate Security per App Category

Regarding RQ3, the survey provided the following results:

H3.1: Users consider different security mechanisms appropriate for different app categories. In Q4, the participants indicated which security mechanisms they regard as suitable to protect their data in the various app categories they use. It was possible to select several mechanisms for one app category. The results are shown in Figure 4. For most app categories, the password is the most frequently chosen security mechanism. However, in the categories social networks and e-mail, users more often selected e-mail & password (30% social networks, 37% e-mail).



	Pass-word	Email & pass-word	PIN	Pattern	Finger print	Face recog nition	Voice recogn ition	TAN proce dure	Smart phone lock	None
Social networks	29	30	11	4	11	3	2	3	6	2
Instant messaging services	28	16	15	6	12	3	2	2	6	9
Email	31	37	8	3	9	3	2	2	4	1
Mobile banking	18	15	21	3	13	5	2	19	3	0
Health/ fitness	29	15	11	8	9	3	2	2	5	15
Mobile shop-ping/ticketing	27	26	13	5	10	4	3	4	4	4
Remote control	25	17	13	6	13	6	5	3	4	7
Dating	33	21	10	6	8	4	2	3	4	8
Cloud services	28	27	12	5	12	4	2	2	4	4

Figure 4. Selection of the appropriate security mechanisms to protect the app categories in question. All values are indicated in percent.

As for mobile banking, the distribution is unusual: 21% opted for the PIN as an appropriate mechanism, 19% for the TAN procedure and only 18% for the password. While the password has generally been chosen most frequently, other security mechanisms are considered more well-suited for specific app categories. Apart from the categories of e-mail and social networks, the mechanism e-mail & password was also considered appropriate for cloud services (27%), mobile shopping/ticketing (26%), and dating (21%). The PIN is, compared to any app category, considered most suitable when using mobile banking (21%). The most unevenly distributed security mechanism is the TAN procedure: 19% of participants chose it for mobile banking, in all other categories it never received more than 4%. The fingerprint reached values of around 10% in most categories, while the pattern was less frequently considered adequate with a maximum of 8% (health / fitness). The least frequently favored measures are face and voice recognition (maximum 6% for remote control). Using the smartphone lock was only viewed as an appropriate authentication method in a maximum of 6% of cases (social networks and short message services). Participants also had the possibility to indicate that they would not use any security mechanism to protect the respective app category. This response received a noticeable number of votes in the health/fitness category (15%), followed by short message services (9%), dating (8%), and remote control (7%). Dating was the category used least often (*I do not use* selected by 47%), followed by remote control (41%), cloud services (34%) and mobile shopping/ticketing (33%).

The Kruskal-Wallis test showed that the distribution of the favored authentication mechanisms for the various app categories is significantly different (H (8) = 289.047, p < 0.0001). H3.1 was thus confirmed. A differentiated view of potential demographic influence factors was omitted due to the complexity of the data and the limited scope of this work.

H3.2: For app categories with more sensitive data, users choose security mechanisms which they perceive to be more secure. To examine the influence of the security assessment on the frequency of selecting a mechanism as adequate for an app category, it was determined how many participants decided in favor of the mechanism being appropriate according to the security assessment (see Table 2). The shares were then considered with respect to the five security levels. It was possible to determine a clear trend regarding the password: 45% of the participants who rated the password as *very secure* chose it as a suitable mechanism for protecting app data. Of the participants who evaluated it as *not secure at all*, only 23% selected it. For other security mechanisms, the trend is not as clear, but the mean of all results shows a similar tendency (18% choose a *very secure* mechanism, while 10% picked one that is *not secure at all*).

	Password	E-Mail & Password	PIN	Pattern	Finger print	Face recognition	Voice recognition	TAN procedure	Mean
Very secure	45%	34%	19%	10%	15%	7%	4%	8%	18%
Fairly secure	41%	36%	20%	10%	13%	4%	6%	7%	17%
Moderately secure	36%	32%	17%	10%	18%	5%	3%	6%	16%
Hardly secure	39%	36%	16%	8%	17%	3%	7%	4%	16%
Not secure at all	23%	27%	13%	3%	5%	2%	3%	5%	10%
Correlation coefficient r Security – Frequency	-0.104	-0.086	-0.105	-0.122	-0.026	-0.117	-0.118	-0.134	
P value	0.001	0.007	0.001	0.000	0.418	0.000	0.000	<0.0001	

Table 2. Shares of the participants who decided on the appropriateness of the security mechanism in dependence of the security assessment and results of the Spearman correlation for perceived security and the frequency of choosing the mechanism as appropriate to protect the app category.

The Spearman correlation was used to test the statistical significance of the trend mentioned above. In this context, the relation between the security assessment of a mechanism and the frequency of it being considered appropriate for an app category was investigated. The results show a low (r = -0,1) [11], yet statistically significant relationship for all security mechanisms except for the fingerprint (see Table 2). The relation is always negative. Due to the encoding of the data (*very secure* = 1, *not secure at all* = 5), this means that mechanisms with higher security are selected more frequently.

To verify whether the selection of security mechanisms is related to the assessment of the need for protection of app data, it was determined which shares of the participants opted for a mechanism, depending on security assessment and assessment of the degree to which app data is worth protecting (see Table 3): 23% of the participants choose a very secure mechanism for an app category that is very protection-worthy. Only 14 % chose mechanisms that are not secure at all in this case. Likewise, only 14% opted for a very secure mechanism to protect an app category that is not protection-worthy at all. The same can be observed for fairly secure mechanisms and app categories fairly protection-worthy. On the other hand, if a category is considered hardly or not protection-worthy at all, no clear trend in the security of the chosen mechanism is apparent. Initially, the results suggest that a secure mechanism is more likely to be chosen for data worthy of protection than for data that is not. However, by means of the Spearman correlation, neither a positive correlation regarding the appropriateness of the mechanisms (r (10155) = 0.145, p < 1), nor a negative correlation regarding the non-appropriateness of the mechanisms (r (46181) = 0.084, p < 1) could be detected; thus, H3.2 is not confirmed.

	Very protection-worthy	Fairly protection-worthy	Moderately protection-worthy	Hardly protection-worthy	Not protection-worthy at all
Very secure	23%	19%	17%	17%	14%
Fairly secure	21%	18%	16%	16%	15%
Moderately secure	19%	18%	15%	14%	14%
Hardly secure	16%	13%	16%	13%	23%
Not secure at all	14%	5%	8%	14%	10%

Table 3. Shares of participants deciding on the adequacy of a security mechanism according to their security assessment and assessment of data sensitivity.

H3.3: Users accept security mechanisms with higher effort in the context of app categories with data worth protecting. As a first step, it was necessary to examine the potential influence of perceived effort on the frequency of selecting a certain authentication mechanism. For this purpose, it was determined how many participants opted for the evaluated mechanism depending on estimated effort (see Table 4). An ambiguous trend is not apparent in the data. For example, the password was least frequently chosen by participants who find it very complex (34%); in contrast, the values were highest regarding PIN (29%), face (10%), and voice recognition (12%).

The mean values of all security mechanisms also show only a weak tendency towards *very complex* mechanisms but are very similar in total. Using the Spearman correlation, only for the fingerprint, a significant correlation could be found between the assessment of effort and the frequency of the mechanism being considered appropriate (see Table 4). Due to the coding of the data (*very complex* = 1, *not complex at all* = 5) the low (r = 0.1) [11] positive correlation can be explained by a positive relationship between little effort and a more frequent selection of the mechanism. Since only one of the eight examined security mechanisms shows a connection between effort and frequency of selection, the assumption that the effort influences the choice of the authentication procedure cannot be confirmed.

	Password	E-Mail & Password	PIN	Pattern	Fingerprint	Face recognition	Voice recognition	TAN procedure	Mean
Very complex	34%	37%	29%	9%	14%	10%	12%	7%	19%
Fairly complex	41%	33%	26%	6%	13%	6%	3%	5%	16%
Moderately complex	39%	32%	19%	9%	15%	4%	2%	5%	16%
Hardly complex	42%	38%	16%	9%	12%	5%	6%	8%	17%
Not complex at all	42%	30%	18%	6%	19%	6%	5%	6%	17%
Correlation Coefficient r Effort – Frequency	-0.001	0.016	-0.044	-0.007	0.106	0.032	0.050	0.044	
P value	0.981	0.614	0.164	0.834	0.001	0.327	0.128	0.179	

Table 4. Shares of the participants who decide on the appropriateness of the security mechanism depending on the effort assessment and results of the Spearman correlation for effort and frequency of selection of the security mechanism as appropriate to protect the app category.

Despite the fact that no general influence could be determined regarding perceived effort of using an authentication mechanism, it was still examined whether there are differences in choice depending on the estimated need for protection of the respective app category. For this purpose, the shares of the participants who decided on the adequacy of a security mechanism depending on the assessment of effort and degree to which data are perceived worth protecting have been determined (see Table 5). The results show that most participants who rated an app category as *very protection-worthy* opted for *a very complex* mechanism (23%). For app categories assessed *fairly protection-worthy*, no trend is apparent. For categories that are *hardly* or *not protection-worthy at all*, it is remarkable that *very complex* mechanisms are chosen most frequently here (22% for *hardly protection-worthy*, 17% for *not protection-worthy at all*). As the results show, no correlation is apparent regarding the choice of security mechanisms that are *very complex* or *not complex at all.* Also, the Spearman correlation between effort and need for protection did not show a correlation for both the appropriateness (r (10155) = 0.035, p < 1) and the non-appropriateness (r (46181) = 0.023, p < 1) of the mechanism. Thus, H3.3 is not confirmed.

	Very protection-worthy	Fairly protection-worthy	Moderately protection-worthy	Hardly protection-worthy	Not protection-worthy at all
Very complex	23%	15%	17%	22%	17%

Fairly complex	19%	19%	16%	14%	16%
Moderately complex	19%	17%	15%	14%	14%
Hardly complex	20%	18%	16%	16%	16%
Not complex at all	20%	20%	17%	13%	12%

Table 5. Shares of participants deciding on the adequacy of a security mechanism according to the assessment of effort and degree to which data are worth protecting.

7 Discussion

Summary and Comparison. The aim of the study was to assess how perceived security and effort regarding security mechanisms, as well as the degree to which app data is seen as worth protecting, influence the choice of appropriate security mechanisms to protect app categories. As the first step, the assessments of security and effort were evaluated. The users saw the fingerprint as the most secure mechanism. This reflects the results of earlier studies, in which the fingerprint was also considered most secure [2, 17, 41].

However, the security assessments of the mechanisms were significantly different in this study, in contrast to those of Zimmermann and Gerber [48]. Our participants rated e-mail & password as well as the TAN procedure as the most complex methods, and fingerprint and PIN as the least complex ones. In contrast to the study by Zimmermann and Gerber [48], the effort assessments of the procedures also differed significantly in our study (H1.2). For the five non-biometric security mechanisms, low positive correlations between estimated effectiveness and effort could be demonstrated. In these cases, greater security is associated with greater effort (H1.3).

Mobile banking is the app category voted as worthiest of protection, followed by e-mail. Conversely, little protection is required for the categories dating and health/fitness. However, the assessments of the need for protection for the various app categories are significantly different (H2). Earlier studies have already shown that especially mobile banking and e-mail are perceived as particularly sensitive: Gerber and Zimmermann [17] identified online banking, online shops and e-mail accounts as the applications on the laptop that are most protection-worthy. Chin et al. [10] reported that respondents are reluctant to retrieve bank data via the smartphone because of its sensitivity, and Egelman et al. [15] showed that an e-mail account contains very sensitive data as well. This also shows the need for context-based protection, as users' find certain data more protect-worthy than other data, which is in line with the results of other studies [19, 30].

In most cases, the participants saw the password or e-mail & password as an adequate security mechanism for protecting an app category. The other authentication mechanisms were rarely chosen. The TAN procedure was remarkably often selected for mobile banking while it was considered appropriate for hardly any other app category. Only in a few cases, the participants deliberately chose no authentication method. Thus, the increasing security awareness of the German population with regard to their smartphone data [12, 43] is also reflected in this study. So far, only a few studies have examined the suitability of different security mechanisms for different application contexts. Gerber and Zimmermann [17] found that using a laptop, particularly in the areas of social networks, cloud services, and e-mail accounts, a text password is much more often preferred to a biometric mechanism in contrast to the participants' general preferences.

This trend cannot be observed in the data available: even though the chosen mechanisms for the various app categories are significantly different (H3.1), password or e-mail & password are always preferred except for mobile banking, while biometric mechanisms generally received lower values. However, this might be due to habits, as users might be more used to these authentication mechanisms.

If we look at the influence of the factors security, effort, and need for protection on the choice of the appropriate security mechanism, it becomes apparent that there is a positive correlation between perceived security and all mechanisms except the fingerprint. Thus, a mechanism that is perceived more secure is more often chosen by participants to protect an app category. However, it has not been proven that an authentication procedure with high attributed security is used especially for app categories which contain highly protection-worthy data (H3.2). The influence of estimated effort on the choice of a security mechanism is low. It was only determined for the fingerprint which was attributed a low effort and used more frequently to protect an app category. The result is unexpected since a high degree of usability was mentioned in several studies as the main criterion for the choice of a security mechanism [14, 27, 41]. When selecting the mechanism, there is no connection between the estimated effort of the security mechanism and the need for protection of the app category (H3.3). This result contradicts that of Ben-Asher et al. [2]. In summary, the choice of the security mechanism is influenced by its perceived security, but not by perceived effort, except for the fingerprint. The need for protection of the app category does not seem relevant. This study therefore shows that users only seem to take the perceived security into account when choosing security mechanisms.

Limitations. To grasp differences regarding the choice of a security mechanism based on perceived security, estimated effort, and assessed value of data we used the Kruskal-Wallis test, thereby viewing the respective values as unpaired even though the same sample was used. Considering the predominant non-correlation of the various factors, one cannot assume it is decisive whether the same person gives multiple answers. But, as there are some results potentially being influenced by using the same sample, it would be plausible to optimize our process by using Friedman's ANOVA for paired values.

The data collected can be used to statistically investigate the impact of security, effort, and need for protection on the adequacy of a security mechanism. However, qualitative surveys are needed to better understand the motivation of respondents to choose a mechanism and to identify other influencing factors. In such surveys [14, 15, 27] , the usability was usually determined as the decisive criterion for the choice of a security mechanism.

Zimmermann and Gerber [17, 48] indicate efficiency, security, data protection, and habit as the most relevant factors. Looking at the results of this study, factors such as habit could justify the frequent choice of the password that otherwise cannot be explained by its perceived security or effort. The remarkably frequent choice of the TAN method in mobile banking also suggests that participants could have selected the mechanisms they currently use to protect the data of the app category. They either actually consider these mechanisms appropriate or they cannot imagine any alternatives. This could be examined further in qualitative investigations.

Conclusion. The study provides two main insights. First, it becomes clear how a representative group of participants assesses security and effort of various security mechanisms, with the fingerprint being the mechanism rated as least complex and most secure; second, it is shown that a positive correlation between estimated security and effort exists for non-biometric authentication procedures. Regarding data sensitivity, significant differences are apparent between the investigated app categories and the choice of the appropriate security methods for the respective category. In this context, the study clearly shows a positive relation between the mechanism's perceived security and its frequency of being selected while hardly any relation to estimated effort of use. Further correlations concerning the need for protection of app data could not be confirmed. This should be considered when designing and choosing app authentication mechanisms: Perceived security of the authentication mechanisms does play the major role for users. Therefore, when designing authentication mechanisms, they should be perceived as secure by users. Hence, users should be considered within the process of choosing an authentication mechanism.

Acknowledgements

This work has been funded by the DFG within the CRC 1119 CROSSING as well as by the German Federal Ministry of Education and Research and the Hessen State Ministry for Higher Education, Research and the Arts within their joint support of the National Research Center for Applied Cybersecurity.

REFERENCES

[1] Aus Online-Shopping wird Mobile-Shopping: 2016. *https://www.bitkom.org/Presse/Presseinformation/Aus-Online-Shopping-wird-Mobile-Shopping.html.*

[2] Ben-Asher, N. et al. 2011. On the need for different security methods on mobile phones. *Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services - MobileHCI '11* (2011), 465.

[3] Benenson, Z. 2012. Attitudes to IT security when using a smartphone. *Computer Science and Information Systems.* (2012), 1179–1183.

[4] Bhagavatula, C. et al. 2015. Biometric Authentication on iPhone and Android: Usability, Perceptions, and Influences on Adoption. *The 2015 Network and Distributed System Security (NDSS) Symposium* (2015).

[5] Bildungsstand: 2016. *https://www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Bildung-Forschung-Kultur/Bildungsstand/_inhalt.html.*

[6] Botha, R.A. et al. 2009. From desktop to mobile: Examining the security experience. *Computers and Security.* 28, 3–4 (2009), 130–137. DOI:https://doi.org/http://dx.doi.org/10.1016/j.cose.2008.11.001.

[7] bpb et al. 2016. *Datenreport 2016. Ein Sozialbericht für die Bundesrepublik Deutschland.* Statistisches Bundesamt.

[8] Buschek, D. et al. 2016. SnapApp: Reducing Authentication Overhead with a Time-Constrained Fast Unlock Option. *Chi '16* (2016), 3736–3747.

[9] Cherapau, I. et al. 2015. On the Impact of Touch ID on iPhone Passcodes. *Soups 2015* (Ottawa, 2015), 257–276.

[10] Chin, E. et al. 2012. Measuring user confidence in smartphone security and privacy. *Proceedings of the Eighth Symposium on Usable Privacy and Security - SOUPS '12* (2012), 1.

[11] Cohen, J. 1992. A power primer. *Psychological Bulletin.* 112(1), (1992), 155.

[12] Das Smartphone ist der beste Freund des Deutschen - Studie von A10 Networks zeigt: Für 70 Prozent sind Apps unverzichtbar: 2017. *https://www.presseportal.de/pm/126713/3643071.*

[13] Deutschland: Mastercard erlaubt Bezahlen per Fingerabdruck und Selfie: 2016. *https://de.ubergizmo.com/2016/10/05/deutschland-mastercard-erlaubt-bezahlen-per-fingerabdruck-und-selfie.html.*

[14] Dörflinger, T. et al. 2010. My smartphone is a safe - The user's point of view regarding graded seurity levels and novel authentication methods. *SECRYPT 2010 - International Conference on Security and Cryptography* (Athens, Greece, 2010).

[15] Egelman, S. et al. 2014. Are You Ready to Lock? Understanding User Motivations for Smartphone Locking Behaviors. *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (2014), 750–761.

[16] Forget passwords and PINs, banks will soon let you access accounts with your VOICE: Santander, HSBC and Lloyds start rolling out audio and video technology: 2016. .

[17] Gerber, N. and Zimmermann, V. 2017. Security vs. privacy? User preferences regarding text passwords and biometric authentication. *Mensch und Computer 2017 - Workshopband: Spielend einfach integrieren* (2017), 279–287.

[18] Grinko, M. et al. Preparation, Recommendations and Warnings: A Representative Survey on the Adoption, Use and Diffusion of Crisis Apps in Germany. *In Mensch und Computer 2019: Tagungsband. ACM, Hamburg, Germany.* 2019.

[19] Harbach, M. et al. 2014. It's a Hard Lock Life: A Field Study of Smartphone (Un)Locking Behavior and Risk Perception. *Proc. of the 10th USENIX Symposium On Usable Privacy and Security (SOUPS).* (2014), 213–230.

[20] Hayashi, E. et al. 2013. CASA: Context-aware Scalable Authentication. *SOUPS '13: Proceedings of the Ninth Symposium on Usable Privacy and Security* (2013), 3:1-3:10.

[21] Hayashi, E. et al. 2012. Goldilocks and the two mobile devices. *Proceedings of the Eighth Symposium on Usable Privacy and Security - SOUPS '12* (2012).

[22] Herley, C. 2009. So long, and no thanks for the externalities: the rational rejection of security advice by users. *Security.* (2009), 133–144. DOI:https://doi.org/10.1145/1719030.1719050.

[23] Hussy, W. et al. 2013. *Forschungsmethoden in Psychologie und Sozialwissenschaften 2. Auflage.* Berlin Heidelberg : Springer-Verlag.

[24] Kaufhold, M.-A. et al. 2018. Avoiding chaotic use of social media before, during, and after emergencies: Design and evaluation of citizens' guidelines. *Journal of Contingencies and Crisis Management.* (2018), 1–16. DOI:https://doi.org/10.1111/1468-5973.12249.

[25] Kaufhold, M.-A. et al. 2019. Potentiale von IKT beim Ausfall kritischer Infrastrukturen: Erwartungen, Informationsgewinnung und Mediennutzung der Zivilbevölkerung in Deutschland. *Proceedings of the International Conference on Wirtschaftsinformatik* (Siegen, Germany, Germany, 2019), 1–15.

[26] Khan, H. et al. 2015. Usability and Security Perceptions of Implicit Authentication: Convenient, Secure, Sometimes Annoying. *Soups 2015* (2015), 225–240.

[27] De Luca, A. et al. 2013. Back-of-device authentication on smartphones. *Proc. CHI* (2013), 2389–2398.

[28] Melicher, W. et al. 2016. Usability and Security of Text Passwords on Mobile Devices. *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems - CHI '16* (New York, New York, USA, 2016), 527–539.

[29] Melicher, W. et al. 2016. Usability and Security of Text Passwords on Mobile Devices. *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems - CHI '16* (2016), 527–539.

[30] Micallef, N. et al. 2015. Why aren't Users Using Protection? Investigating the Usability of Smartphone Locking. *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services - MobileHCI '15* (2015), 284–294.

[31] Mobile Steuerungszentrale für das Internet of Things: 2017. *https://www.bitkom.org/Presse/Presseinformation/Mobile-Steuerungszentrale-fuer-das-Internet-of-Things.html.*

[32] Muslukhov, I. et al. 2013. Know Your Enemy: The Risk of Unauthorized Access in Smartphones by Insiders. *Proceedings of the 15th International Conference on Human-Computer Interaction with Mobile Devices and Services (MobileHCI '13)* (2013), 271–280.

[33] Muslukhov, I. et al. 2012. Understanding users' requirements for data protection in smartphones. *Proceedings - 2012 IEEE 28th International Conference on Data Engineering Workshops, ICDEW 2012* (2012), 228–235.

[34] Muzammal, S.M. et al. 2016. Conceivable security risks and authentication techniques for smart devices: A comparative evaluation of security practices.

International Journal of Automation and Computing. 13, 4 (2016), 350–363. DOI:https://doi.org/10.1007/s11633-016-1011-5.

[35] Mylonas, A. et al. 2013. A qualitative metrics vector for the awareness of smartphone security users. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. 8058 LNCS, (2013), 173–184. DOI:https://doi.org/10.1007/978-3-642-40343-915.

[36] Payne, B.D. and Edwards, W.K. 2008. A brief introduction to usable Security. *IEEE Internet Computing*. 12, 3 (2008), 13–20. DOI:https://doi.org/https://doi.org/10.1109/MIC.2008.50.

[37] Pocovnicu, A. 2009. Biometric Security for Cell Phones. *Informatica Economica*. 13, 1 (2009), 57–63. DOI:https://doi.org/http://revistaie.ase.ro/content/49/006-Pocovnicu.pdf.

[38] PwC-Umfrage: Mobile Payment in Deutschland auf dem Vormarsch: 2015. *https://www.pwc.de/de/digitale-transformation/mobile-payment-in-deutschland-auf-dem-vormarsch.html*.

[39] Reuter, C. et al. 2019. Fake News Perception in Germany: A Representative Study of People's Attitudes and Approaches to Counteract Disinformation. *Proceedings of the International Conference on Wirtschaftsinformatik (WI)* (Siegen, 2019).

[40] Reuter, C. 2018. *Sicherheitskritische Mensch-Computer-Interaktion: Interaktive Technologien und Soziale Medien im Krisen- und Sicherheitsmanagement*. Springer Vieweg.

[41] Sari, P.K. et al. 2016. An evaluation of authentication methods for smartphone based on users' preferences. *IOP Conference Series: Materials Science and Engineering*. 128, 1 (2016). DOI:https://doi.org/https://doi.org/10.1088/1757-899X/128/1/012036.

[42] Shafique, U. et al. 2017. Modern Authentication Techniques in Smart Phones : Security and Usability Perspective. *(IJACSA) International Journal of Advanced Computer Science and Applications*. 8, 1 (2017), 331–340. DOI:https://doi.org/https://doi.org/10.14569/IJACSA.2017.080142.

[43] Smartphone-Nutzer gehen auf Nummer sicher: 2016. *https://www.bitkom.org/Presse/Presseinformation/Smartphone-Nutzer-gehen-auf-Nummer-sicher.html*.

[44] Statistisches Bundesamt 2016. *Bevölkerung Deutschlands nach Altersgruppen 2016*. Statista.

[45] Trewin, S. et al. 2012. Biometric authentication on a mobile device: a study of user effort, error and task disruption. *Proceedings of the 28th Annual Computer Security Applications Conference, (ACSAC '12)* (2012), 159–168.

[46] Volkamer, M. et al. 2015. A Socio-Technical Investigation into Smartphone Security. *11th International Workshop (STM 2015)* (2015), 265–273.

[47] XLSTAT: 2017. *https://www.xlstat.com/de/*.

[48] Zimmermann, V. and Gerber, N. 2017. "If it wasn't secure, they would not use it in the movies" – Security perceptions and user acceptance of authentication technologies. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (2017), 265–283.