Fingerprint Recognition on Mobile Devices: Widely Deployed, Rarely Understood

Farzaneh Karegar
Karlstad University
Karlstad, Sweden
farzaneh.karegar@kau.se

John Sören Pettersson
Karlstad University
Karlstad, Sweden
john_soren.pettersson@kau.se

Simone Fischer-Hübner
Karlstad University
Karlstad, Sweden
simone.fischer-huebner@kau.se

ABSTRACT

Only a few studies have addressed the users' conception of how fingerprint recognition used for different purposes on mobile devices works. This study contributes by investigating how different groups of individuals think that the fingerprint recognition works, why they think so, and also by pointing out differences in pin code and fingerprint issues. The study furthermore yields some results concerning individuals' attitudes towards how sensitive the use of fingerprint sensors is: non-users tended to be more afraid of third-party access than users. On the other hand, users tended to regard the fingerprint pattern as more sensitive than non-users.

This study also manages to give some methodological contributions, namely that mockup user interfaces do not bias the parameters studied in this paper (e.g. understanding of access to fingerprint data), and that self-estimation of knowledge in Computer Security is not a good indicator of respondents' understanding of fingerprint security and privacy. Moreover, people who connected a low degree of sensitivity to fingerprint patterns gave very different reasons for their estimation of sensitivity. This prompts for more research, as it is unclear if different groups would benefit from different information and modes of visualisation to understand what are the issues involved in fingerprint recognition on mobile devices.

CCS CONCEPTS

• **Security and privacy** → **Social aspects of security and privacy**; *Privacy protections*; Usability in security and privacy;

KEYWORDS

Fingerprint Pattern, User Perception, Sensitive Information, Data Privacy

ACM Reference Format:

Farzaneh Karegar, John Sören Pettersson, and Simone Fischer-Hübner. 2018. Fingerprint Recognition on Mobile Devices: Widely Deployed, Rarely Understood. In *ARES 2018: International Conference on Availability, Reliability and Security*, August 27–30, 2018, Hamburg, Germany. ACM, New York, NY, USA, 9 pages. <https://doi.org/10.1145/3230833.3234514>

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

ARES 2018, August 27–30, 2018, Hamburg, Germany

© 2018 Association for Computing Machinery.

ACM ISBN 978-1-4503-6448-5/18/08...\$15.00

<https://doi.org/10.1145/3230833.3234514>

1 INTRODUCTION

Research on users' perceptions and attitudes toward security, usability, social acceptance, and adoption of different biometric recognition systems abound (e.g. [4], [6], [9], [10]). The most well-known biometric recognition systems are fingerprints, iris, face, and voice recognition, among them, the highest acceptability is gained for fingerprint recognition [19]. The introduction of fingerprint recognition on mobile devices is among the first large-scale deployments of biometrics for consumers [4].

Fingerprint recognition integrated into many smartphones today can counter security issues (e.g. guessing and brute force attacks) and usability issues (e.g. memorizing some information) inherent in traditional secret-knowledge-based solutions such as passwords, pin codes, and pattern locks. Fingerprint recognition can also be used as a second authentication factor for improved security. However, fingerprint biometrics present sensitive personal data that may also raise privacy concerns. Fingerprint recognition is used both for unlocking a smartphone and for other critical functionalities in the smartphone, for example, for approving transactions in financial applications. Swedish Mobile BankID app¹ and the Identity Wallet app developed in the CREDENTIAL EU project² are examples of modern apps which allow users to use fingerprint recognition for authenticating to third-party services, approving payments or confirming contracts and consents. Fingerprint recognition involves revealing the users' sensitive biometric data to mobile devices which should not be distributed further to other entities. Regarding the importance people attach to the collected authentication data, fingerprint information seems most critical for people compared to data for face, voice, and iris recognition and traditional pin code/password authentication, according to a study reported in [24]. In contrast, storing the password or pin seems least critical for the respondents [24]. In 2015, Bhagavatula et al. reported that worries that biometric data would be sent to the cloud, rather than constrained to the device itself, could be a barrier to adoption for users [4]. Best practice privacy guidelines for biometrics [17] are therefore suggesting to store biometric data on the user's device under her control if possible.

Nowadays, iOS and Android operating systems are designed based on the principle of keeping the secure data on a part of the processor that cannot be accessed by apps operating in the regular operating system environment. For example, Secure Enclave on iOS mobile phones [2] and Trusted Execution Environment (TEE) on Android phones [21] (e.g. using ARM Trustzone) are the only locations where the fingerprint authentication process takes place on modern secure mobile devices. In other words, fingerprint data

¹<https://www.bankid.com/en/om-bankid/detta-ar-bankid>

²EU H2020 project CREDENTIAL (Secure Cloud Identity Wallet), www.credential.eu

are saved and processed only locally without being accessed by any applications. Nonetheless, previous studies [15] [14] from which our paper stems showed that users' perception of fingerprint access and storage is not compatible with current implementations.

For this paper, we conducted an online study (i.e. an Internet-based survey) with 100 participants to investigate individuals' perception of privacy of fingerprint recognition on mobile devices and sensitivity of fingerprint data. Our work contributes to the body of knowledge by reporting and discussing 1) people's perception of entities which have access to and control of authentication tokens (i.e. fingerprint biometric data vs. pin codes) in the context of Identity Providers (IdPs), 2) the differences in attitudes towards privacy and sensitivity of fingerprint data between people who actually use the fingerprint technology on their devices and others, and finally 3) people's subjective opinions about the degree of sensitivity of fingerprint data and their justifications of their answers. Investigating users' perception of access to and storage of fingerprint data as sensitive data (i.e. perception of privacy) and users' opinions about its security can help system and User Interface (UI) designers to address users' problems. Future systems should be better at helping people to make informed decisions about the authentication methods.

In the next section, we present the background of biometric fingerprint authentication for mobile apps on mobile devices. Section 3 presents the related work. The methodology and study design are presented in the Section 4, while Section 5 presents the main results, and Section 6 reports and discusses findings related to fingerprint sensitivity. Section 7, finally, puts the discussion in the general context of biometrics and authentication to IdPs.

2 BACKGROUND

2.1 Sensitivity of Fingerprint Biometrics

Art. 9 of the EU General Data Protection Regulation (GDPR) includes biometric data used for identification purposes as one of the "special categories" of data that are per se very sensitive and need special protection. Previous research has shown that sensitive information about the user's cognitive abilities or sexual orientation could be derived from fingerprint patterns [8], [16], or have a social stigma and may even carry a "racial overtone" in certain countries, such as the UK [11].

For these reasons, there are best practice guidelines of how biometrics should be handled in a privacy-respective manner that also suggest storing the biometric data on the user's device under her control if possible (see [20], [17]).

Moreover, control over biometric data by the individual user has almost become a requirement for privacy compliance for some national Data Protection Authorities [17], [18]. Apart from privacy issues, the unforgeability and authenticity of fingerprint patterns are also critical from a security perspective.

2.2 Processing of Fingerprint Patterns

How fingerprint recognition works on current mobile devices. Here we briefly describe how fingerprint recognition used for different purposes (e.g. unlocking the phone or authenticating

to other apps) works in general without describing the technical details which are out of the scope of this paper.³

In current modern smartphones equipped with fingerprint sensors, the fingerprints taken from people (i.e. fingerprint images) are stored encrypted in the device after being translated into a mathematical representation (i.e. templates). However, in our questionnaire, to hide technical details from users, we did not distinguish between the terms fingerprint image (scanned fingerprint pattern) which is temporarily stored in TEE or the Secure Enclave (to derive the template of each fingerprint query) and fingerprint template that is finally stored as one enrolled template on the device.⁴

When a user wants to unlock the device using the fingerprint sensor the query template is then compared to the enrolled template(s) to identify a match and unlock the device. Scanned fingerprint or enrolled template cannot be accessed by the OS on the device or by any applications running on it.⁵ It cannot either be used to match against other fingerprint databases in other devices and it is not possible for someone to reverse engineer the actual fingerprint image from the stored template. Also, for authenticating to third-party apps, the apps just receive whether a fingerprint has been verified or not.

The importance of proper comprehension of handling fingerprint data. If people do not understand that fingerprint data is processed and stored locally on their devices, under their control, they may have privacy concerns and it may prevent them from adopting this technology and benefiting from its features. Although De Luca et al. reported that usability is one of the main factors that influence the decision on whether or not to use biometric authentication on smartphones among US residents [6], Zimmerman and Gerber [23] concluded in their study that for selecting the authentication method, including biometrics, privacy plays an important role. According to [23], some people prefer passwords for privacy reasons⁶ and some prefer biometrics for the perceived security of using its unique features.

Finally, misunderstanding of access to authentication token will have some effects on obtaining and withdrawing consent, especially in the context of IdPs. Right to withdraw consent is given much emphasis in the GDPR besides other requirements on informed consent. Article 7(3) of the GDPR prescribes that the controller must ensure that consent can be withdrawn by the data subject as easy as giving consent and at any given time. The GDPR does not require that giving and withdrawing consent must always be done through the same action. If fingerprint recognition is used for confirming consent or contracts on mobile devices, to effectively exercise the right to withdraw consent, users should not think that they are endangering a piece of their sensitive personal data (i.e. their fingerprint pattern) to stop processing of their other personal data. Therefore, it is of high importance for designers to decide which method they select to assure obtaining informed consent

³Interested readers can refer to [21], [2].

⁴Also, distinguishing between these two concepts does not affect the fact about who has access to them.

⁵Note that the ultimate security and privacy of the fingerprint data depend on how TEE is implemented. There might be some design issues affecting the security of some devices: <https://googleprojectzero.blogspot.com/2017/07/trust-issues-exploiting-trustzone-tees.html>.

⁶Because they believe no personal data is used and consequently no personal data can be stolen.

from the right individual and also cancelling the consent for the same individual without causing them to believe that even for canceling their consent they disclosed a piece of (sensitive) personal information.

3 RELATED WORK

Our work in this paper is very much related to the work conducted by Karegar et al. [15] and Javed et al. [14] which investigated about users' perception regarding access and storage of fingerprint data on mobile devices. This paper has its background in the results of those aforementioned studies [15] [14] and in some difficulties to make screen mockups to work fully natural in the CREDENTIAL project.

In [15], authors tested the general UIs of the CREDENTIAL Wallet⁷ app (see [12] for the detailed structure of CREDENTIAL Wallet architecture). In order to detect test participants' use of the fingerprint scanner, they asked them to click on the screen for the mockup. The analysis of post-test questionnaires revealed that many test participants had an erroneous idea that the fingerprint pattern was forwarded to the IdP app [15] (which might be explained by the interactive mockup construction). Some also believed that the fingerprint pattern was shared with the service provider to which the user was asked to register and later sign in using the CREDENTIAL as an IdP. Some participants (residents in Sweden) were very familiar to an advanced IdP called Mobile BankID. There was a significant tendency that these participants thought that their fingerprint pattern was shared with other entities involved in the scenario rather than just the mobile device itself. This could be a matter of trust: as users trust their banks to have safe solutions, there is no reason for these users do not assume that the BankID app handles also the fingerprint authentication. However, one could argue, there could have been a misleading influence for the other participants not resident in Sweden to rely on the pin code concept to understand fingerprint processing. Perhaps this could explain some of the erroneous answers from a few of the participants not using the Swedish BankID.

Javed et al. [14] investigated users' comprehension and risk perception of Apple's Touch ID technology in the context of Amazon in-app purchasing using the fingerprint sensor on mobile devices. Their findings showed that at least 50% of people who have iOS devices with fingerprint sensors (Javed et al. referred to them as users of Touch ID) are unaware of the Touch ID authentication process for signing into the apps (they believe fingerprint authentication is the same as username/password authentication). They also showed that users of Touch ID have incorrect perceptions regarding the storage and access of registered fingerprint during the Touch ID authentication (they believe that Amazon's app used their fingerprint to authenticate them.), and do not have a proper comprehension of ease of bypassing Touch ID technology [14]. Nonetheless, it is not clear if Javed's et al. participants were really using the fingerprint sensors on mobile devices and how the results would change with non-users. Further, to investigate if users' perception of fingerprint

authentication was equivalent to username/password authentication they asked a vague question: "Is being authenticated by your fingerprint the same as by your username/password?" without clarifying the aspects on which they are focusing to highlight the difference. The question does not assure the conclusion derived from participants' answers. Participants could answer by selecting "Yes", "No", and "I do not know". However, if they said "Yes" it would not necessarily assure that they did not know about the differences in underlying process (e.g. who has access to their authentication tokens) but simply they might have thought about the result of the authentication process which could fail or pass them in both cases (note the "is being authenticated" in the question). Likewise, answering "No" could refer to different UIs they would experience on their phones in both processes.

Considering the issues discussed in this section and some limitations of studies conducted by Javed et al. [14] and Karegar et al. [15], we designed an online study to investigate different people's (users and non-users of fingerprint sensors and familiar and non-familiar with similar IdP technologies) perception of privacy of authentication tokens (i.e. both fingerprint and pin code) in the context of IdPs and their perception of sensitivity of the fingerprint data.

4 METHODOLOGY

We designed four videos that our participants watched in an online study in which a user signs up for a service using an IdP. To investigate the possible effects of familiarity with similar technologies (e.g. Swedish Mobile BankID) on users' perception regarding fingerprint, we have two different IdPs in our videos. In two videos (VCP and VCF), we have the CREDENTIAL Wallet as the IdP accessible via a mobile app and in two others (VBP and VBF) we have the Swedish Mobile BankID as an IdP. Further, to see if the users' perception of the fingerprint pattern processing differs from their understanding of pin code processing, we included two scenarios: the user in the videos accepts the request of the service provider in an authorization dialogue by either 1) entering her pin code in VBP and VCP, or 2) scanning her fingerprint in VCF and VBF.

The videos were included in an online questionnaire made using Surveygizmo⁸ platform. We distributed the link to the questionnaire via mailing lists and social media. Participants were supposed to first watch one of the videos and then answer some questions. However, they were not randomly assigned to one of the four videos. A question about whether they have ever experienced Swedish Mobile BankID helped to assign the ones who say "YES" to videos with the Swedish Mobile BankID as the IdP and the others to the videos having the CREDENTIAL wallet app as the IdP.

Further, in order to randomly assign participants to show them a video with the pin code or with the fingerprint scanning, we asked them to answer whether they were born in the first six months of a year (January to June) or in the last six months (July to December). Based on their answers to this question we assigned them to pin code or fingerprint videos.

Each of the CREDENTIAL videos is 1 minute and 49 seconds while each of BankID videos is only 57 seconds long because the respondents seeing the BankID videos were already familiar with

⁷The CREDENTIAL wallet performs authentication and authorization processes. It supports users with its functionality through a mobile application which offers them to use fingerprint recognition for authentication and other services.

⁸<https://www.surveygizmo.eu/>

the IdP in the video and, moreover, in the BankID videos the user is not supposed to select personal information to be shared with the service provider. On average, it took approximately 8 minutes for participants who watched BankID videos and 10 minutes for participants who watched CREDENTIAL videos to finish the survey⁹. Participation was voluntarily without any compensation. Participants first read and accepted the consent form and then participated in the survey.

4.1 Questions in the Study

In our study, after answering two questions for assigning people the video to watch, individuals were asked to watch the video and then answer some questions about their use, understanding, concerns and attitudes of authentication methods. First, we asked people about the entities they think have access to their fingerprint pattern or pin code in the context shown in the videos they watched. This question was a multiple-choice question where participants could select as many as entities that apply (and the combination) of the following: the mobile device, the (CREDENTIAL Wallet/Mobile BankID) app, and the website (for which the user in the video wanted to sign up). Then people were asked to justify why they think the selected entities have access to their fingerprint patterns.

Not all mobile devices have fingerprint sensors and not all users may have used the fingerprint sensor on their devices. Therefore, we asked people if they ever used fingerprint sensors on their devices. We used the answers to this question to investigate the differences between users and non-users. For participants who never used the fingerprint sensor on their devices, we asked them about the reason of not using it (open question) and if they were using some other techniques to unlock their devices, including *slide to unlock*, pin code, password, pattern, and none. For participants who used fingerprint sensor we asked when for the first time they activated it and for what purposes they used their fingerprint sensors, providing them three alternatives to select among: for unlocking the mobile device, authenticate transactions on the phone (e.g. Google or Apple Pay) and unlock mobile apps on their phones. There was also a text field to enter other answers to this question.

All participants were asked some questions regarding how they perceived or understood the sensitivity, security and privacy of fingerprint pattern data. Specifically, we asked them to give their subjective opinions about three statements presented in Table 1 by giving them a rank from 1 (Strongly Disagree) to 10 (Strongly Agree). The answers to these questions are reported in Section 6, while the possible differences between different user groups are reported in Section 5.

Finally, the questionnaire requested for some demographic data, as explained in the next subsection.

According to the Swedish *Ethical Review of Research Act* (Etikprövningslagen), no ethical review and approval for our survey was required, as we did not collect any special categories of data (i.e. no “sensitive data” as defined in Etikprövningslagen and the GDPR) and followed the data protection rules of the Swedish Data Act (PUL) and the GDPR. In particular, we obtained informed consent in conformance with PUL and the GDPR by all volunteering participants.

⁹The time includes both watching the video and answering the questions.

4.2 Demographics

In total, we received 100 online participants in the period we set for collecting data from the beginning of September 2017 to the end of November 2017. Fifty-one of them watched BankID videos (26 with fingerprint and 25 with pin code) and 49 watched CREDENTIAL (28 with fingerprint and 21 with pin code) videos. We had 40 females and 56 males while four participants preferred not to answer the gender question. Among our 100 respondents, 44 never used authentication by fingerprint. Table 2 shows an overview of the demographics of this study.

5 PERCEPTION OF ACCESS TO THE AUTHENTICATION TOKENS

First, in this section, we report about our results regarding 1) whether users’ perception differs for the access to pin code and fingerprint pattern in the context of IdPs, and 2) the conjecture for the role of familiarity with the IdP on users’ perception about access to authentication tokens (i.e. fingerprint and pin code). We have two null hypotheses:

H₀1. There is no relationship between correct perception of access to authentication tokens and type of method used to give consent, i.e. pin code and fingerprint, in the context of IdPs.

H₀2. There is no significant difference between people who do not use Swedish mobile BankID and people who use such trusted IdPs regarding their awareness of entities who access their authentication tokens in the context of IdPs.

Then, we report our further findings and discussions regarding the relationship between perceptions of access (privacy of authentication tokens) and level of self-estimated knowledge in Computer Security.

Besides indicating which entities have access to the authentication tokens in the context of the authorization scenarios shown in the videos, participants were requested to justify their answers. As discussed above, the fingerprint pattern is only accessed by the mobile device, not other entities such as mobile apps or service providers. However, the pin code is mainly accessed by the mobile app (i.e. CREDENTIAL app and BankID app) in which users enter their pin codes and one can argue that the pin code is also accessed by the mobile phone, for example, the running operating system and its keyboard. To analyse users’ answers who watched the videos involving using pin codes, we considered also how they justified their answers. Based on their justifications, the answers that pin code is accessed by mobile app and mobile devices are considered as wrong or right answers. In total, 20 participants believed that the mobile app and the mobile device accessed the pin codes, among them, seven provided meaningful justification and their answers were coded as correct (see Table 3 for answers considered correct).

5.1 Hypotheses Testing

To test H₀1, we used Chi-Square Test of Independence and we could reject the hypothesis about independence: $\chi^2(1) = 4.162$, $p = 0.041$. Twenty-nine (29) of 49 participants who watched pin code videos answered correctly about who accessed pin code comparing to the 54 participants who watched fingerprint videos and just 23 answered correctly that the mobile device had access to it. Approximately 43% of participants who watched fingerprint videos had

Table 1: Summary of answers to questions regarding sensitivity, security and privacy of the fingerprint pattern.

Type of IdP in video	Technique used in video		Q1. I believe that the fingerprint pattern is really sensitive information.	Q2. I consider using the fingerprint pattern more secure than other security measures (e.g. a pin code , a password)	Q3. I would be concerned that fingerprint pattern,could be distributed, shared, or accessed by a third party.
BankID	Fingerprint	Mean	6.73	5.73	7.19
		Std. D.	2.15	2.71	2.83
	Pin code	Mean	6.40	4.88	6.88
		Std. D.	1.96	2.79	1.94
CREDENTIAL	Fingerprint	Mean	7.54	6.89	8.57
		Std. D.	2.24	2.86	2.25
	Pin code	Mean	6.57	6.38	8.19
		Std. D.	2.98	2.77	1.99
Total	All (N = 100)	Mean	6.84	5.98	7.71
		Std. D.	2.33	2.85	2.37

a correct view of who accessed it (23 out of 54). Therefore, we reject our conjecture that may arise from the results of the study in [15] that just the conditions of the mockup for faking fingerprint-scanning (click on an icon on the screen) misled users to think that fingerprint is accessed by other entities. Consequently, for simplified UIs in the user studies which do not measure the exact characteristics of fingerprint sensors (e.g. how much it takes people to authenticate using fingerprint sensor), clicking on an icon on the screen would be a proxy of using fingerprint sensors on mobile devices.

We also used Chi-Square test of independence to test H_02 and to see whether the group using Mobile BankID in daily life and the others (seeing CREDENTIAL) differ from each other. We could not reject the H_02 hypothesis.¹⁰ Therefore, our results did not show any relationship between the understanding of access to authentication tokens and using (or not using) Swedish Mobile BankID app. Contrary to the results reported in [15], in our sample, participants' knowledge could have counteracted the effects of trust in familiar IdPs on access-belief. This would explain why, in our sample, the effect of using Swedish Mobile BankID, an IdP in which users trust, did not show any significant influence on access-belief as compared to "the others" (here: the respondents who saw the CREDENTIAL videos). As most of our participants ($n = 80$, see Table 2) reported that they have some knowledge of Computer Security, it can be assumed they are not nontechnical people in contrast to the respondents in [15].

5.2 Self-estimated Security Knowledge not Relevant for Mobile Authentication Processes

We found a significant evidence of relationship between the correct perception of access to authentication tokens and the level of self-estimated knowledge about Computer Security using Fisher's Exact Test of Independence¹¹ with $p = 0.021$. (We removed the "Other" option in the question about Computer Security knowledge as just one participant selected that and it does not give a meaningful view of the participant's knowledge.)

¹⁰The significance level $\alpha = 0.05$ but the calculated $p > 0.05$.

¹¹We used Fisher's Exact Test of Independence instead of Chi-Square Independence Test because more than 20% of cells had expected frequencies < 5 .

This relationship is very apparent in Figure 1 where the "No knowledge" group is the only group where more respondents had a wrong notion than a correct notion about who has access to authentication tokens. However, a post-hoc test (e.g. cf. [7] and [3]) did not show any clear evidence regarding the individual groups' contribution to the overall relationship. Although there is no statistically significant pattern among the different groups in the contingency table, participants who reported themselves as having no knowledge in Computer Security often had an incorrect view regarding access to authentication tokens comparing to others ($p = 0.00790$)¹².

Nevertheless, in spite of the result of the Fisher's Exact Test and the dominance of incorrect views among the "No knowledge" respondents, Figure 1 shows there are notable proportions in the three other groups that held incorrect views too. Thus, participants who report higher level of knowledge in Computer Security do not necessarily have knowledge and a good perception about a specific security phenomenon such as security and access to fingerprint pattern and pin code of apps. Eleven of 33 participants who reported that they are professionals in Computer Security or are quite familiar with Computer Security provided wrong answers to the question about access to authentication tokens. In Table 4, we report some of their justifications for their wrong answers.

6 VALUATION OF FINGERPRINT AUTHENTICATION BY USERS AND NON-USERS

In our study, we asked all participants if they ever used the fingerprint sensor on their mobile or tablet devices. Therefore, we can identify which respondents actually have some familiarity of fingerprint sensors when we interpret answers to the other questions. Our analysis of the participants' answers shows that there is no relationship on the level of $p < 0.05$ between being the user of the fingerprint sensor and the perception regarding who has access to it. Therefore, we assume that the current procedures to activate and use fingerprint sensors do not help smartphone users to gain a correct view of the privacy and processing of their fingerprint pattern (i.e. who has access to it).

¹²This is the p value associated with adjusted residuals in the contingency table; the Bonferroni corrected p value is $0.05/8 = 0.00626$.

Table 2: Demographic information

Demographic info	VBFB (n=26)	VBFB (n=25)	VCF (n=28)	VCP (n=21)	Total (n=100)
Gender					
Female	10	12	10	8	40
Male	16	12	16	12	56
Preferred not to say	0	1	2	1	4
Age					
18-24	2	1	2	1	6
25-34	8	5	9	9	31
35-44	7	14	10	5	36
45-54	7	3	5	4	19
55-64	0	1	2	2	5
65-74	2	1	0	0	3
74+	0	0	0	0	0
Country they live in					
Sweden	25	25	0	0	50
Germany	0	0	3	8	11
Spain	0	0	15	9	24
Austria	0	0	3	2	5
Other (7 Cont. Europe + 2 UK + 1 US)	1	0	7	2	10
Ever used fingerprint sensor on mobile or tablet devices?					
YES	19	16	13	8	56
NO	7	9	15	13	44
Purpose of using fingerprint sensor on mobile or tablet devices					
Not applicable (Never used it)	7	9	15	13	44
Unlock mobile device	7	2	2	5	16
Unlock mobile apps	1	0	2	0	1
Unlock mobile device and unlock mobile apps	2	7	4	0	13
Unlock mobile device and authenticate transactions	3	5	2	1	11
Unlock mobile device, unlock mobile apps, and authenticate transaction on phone	6	2	5	2	15
What they mainly use instead of fingerprint on their mobile or tablet devices					
Not applicable (they use fingerprint)	19	16	13	8	56
None	1	0	2	1	4
Slide to unlock	3	1	1	4	9
Pattern	0	2	7	3	12
Pin code	2	4	3	5	14
Password	0	2	2	0	4
Other	1	0	0	0	1
Knowledge in Computer Security (Respondents' self-estimation)					
No knowledge	7	6	4	3	20
A bit familiar	12	16	7	11	46
Quite familiar	7	2	10	3	22
Professional	0	1	7	3	11
Other	0	0	0	1	1

Potentially, one could go further with our set of respondents to see if non-users are more prone to certain other conceptions of fingerprint authentication than users, especially the sensitivity, security, and privacy regarding the fingerprint pattern. However, the reason for why people do not use a fingerprint sensor might be that there simply is no sensor on their mobile phone. Forty-four

Figure 1: Number of participants categorised based on their perception of access to authentication tokens and their Computer Security knowledge (self-estimated)

of our participants never used fingerprint sensors on their devices. Among them, 17 do not use it for other reasons than that it is not available on their mobile or tablet devices. Of these 17, seven people did not trust it or found it complicated.

For the question “I consider using the fingerprint pattern more secure than other security measures (e.g. a pin code, a password)” (Q2 in Table 1), we could not establish a significant evidence of the relationship between using the fingerprint sensor and perception of its security. In accordance with the results reported in [14] and [4], our participants believed fingerprint measure is more secure than other security measures such as passwords and pin codes. However, current implementations of biometric authentication cannot be more secure than a pin code or a password because a password, for example, is always used as a fallback mechanism.

The Kruskal-Wallis-Test¹³ showed that there is a significant difference between using (and not using) a fingerprint sensor and concerns about third-party access (Q3 in Table 1), $\chi^2(1)=4.747$, $p=0.029$, with the 44 non-users being more concerned about third-party access (mean = 6.64, SD = 3.00) than users (mean 5.46, SD = 2.63). On the other hand, there is a significant difference between using (and not using) fingerprint and attitudes towards the sensitivity of fingerprint data (Q1 in Table 1), $\chi^2(1) = 3.899$, $p = 0.048$, with non-users (mean = 7.20, SD = 2.47) tend to see fingerprint patterns as less sensitive than users do (mean = 8.11, SD= 2.23). There is no contradiction between the use of fingerprint sensor and a belief that fingerprint pattern is really sensitive information. Any token used for authentication is a sensitive piece of information from a security perspective. For instance, a pin code is also a “really sensitive information”, at least for a person who uses pin codes.

6.1 Reasons Given for Sensitivity of Fingerprint Pattern

Besides asking participants to tell us to what extent they think that a fingerprint pattern is sensitive data, they were requested

¹³We used non-parametric tests since the assumptions of normality and homogeneity of variances were violated.

Table 3: Justification of why pin code is accessed by mobile app and mobile device considered as right answers.

Type of Video	Justifications for why pin code is accessed by mobile device and app
VCP	Mobile device from keyboard input (OS/drivers). App because it should use the PIN somehow.
VCP	The app is clear because it needs to verify that the pin is correct. The mobile device can have access in case the pin pad keyboard is the general keyboard of the OS and is not a secure keyboard inside the app.
VBP	Device: the device should in some way have access to everything I do on my device. App: I enter the code into the app which authenticates it. It has direct access to my code.
VBP	The app would have as it will value if the code is correct, and perhaps my device can also "see" the code, I will not presume otherwise anyway.
VBP	The device keyboard app receives the button presses and a malicious keyboard or accessibility app can log these. The bankid app uses the pin code to unlock the certificate in the device.
VBP	The mobile can keep the keystrokes, and also it sends them to the application. BankID has to check the pin code (or the hash of the code) to authenticate, the user.
VCP	The mobile device is the input device and therefore "knows" what I am typing. The CREDENTIAL Wallet app is the service which I am using to identify myself and therefore needs to know if the pin that I entered is correct.

Table 4: Examples of wrong perceptions among people with Computer Security knowledge about authentication token access.

Type of video	Access to authentication tokens	CS level	Reason
VBF	Mobile device and app	Quite familiar	I think the mobile device sends it to the bank-id app who also has the fingerprint and compares them and let me in to the service if they match.
VCF	Mobile device and app	Quite familiar	the fingerprint pattern is introduced in the mobile device, and the CREDENTIAL Wallet app needs to store it in order to validate the fingerprint pattern which is trying to log into the app
VCP	Mobile device, app, and website	Quite familiar	The moment I have keyed in my PIN into any electronic device, I have lost control over its security. I have no way to know if or where it is stored or sent or used
VCF	Mobile device and app	Professional	I think the mobile device has access to the fingerprint because it is the device being used for reading it. The credential wallet app needs to access the pattern of the fingerprint to check my identity
VCF	Mobile device and app	Professional	These are the entities where the fingerprint is taken and verified. But it's not required on the website side
VCP	Mobile device and app	Professional	Security

to describe the reasons for the answer they provided in an open text format. We analysed the reasons they provided for the level of subjective sensitivity of a fingerprint pattern.

In total, 22 participants rated the sensitivity 5 or less on the 1-10 scale provided in the questionnaire. The most common reasons for their answers are as follows. Some participants mentioned that the fingerprint pattern is available everywhere they touch so it cannot be hidden. Some participants justified their low perception of sensitivity based on the fact that fingerprint is difficult to be forged, hacked, or replicated. Interestingly, contrary to this group,

some said it is easy to be forged, hacked, or replicated, therefore, it cannot be very sensitive. The reason and implications behind this conflict need more investigation. Would the two groups benefit from different information to understand when the fingerprint is a secure (or risky) option?

Lack of knowledge about the potential misuses or lack of ability to imagine bad scenarios, lack of ability to identify the person by just the pattern (as believed by some participants)¹⁴ and the belief that it does not contain personal information were among the other reasons mentioned by participants which caused them to rate the sensitivity low. Nobody mentioned that other personal information, besides identity, could be derived from the pattern itself.

Fingerprint pattern cannot be derived from other sets of information¹⁵, as also mentioned by one of the participants. On the other hand, the pattern itself can reveal more sensitive data about individuals according to some authors ([8], [16],[13]). However, as noted, no respondent mentioned this possibility. In Q1 we did not distinguish between digital images of fingerprint patterns or the physical patterns left on several substances. Nonetheless, whether from digital patterns or from physical patterns, more characteristics could be derived. Therefore, it does not affect our results that it is not possible to say that all 100 respondents had the same idea of "fingerprint pattern."

Some participants also did not distinguish between the fingerprint pattern and other security measures and rated it low, as they believed it is not more sensitive than other information. Among the 22 participants who rated the fingerprint low (5 or less) regarding its sensitivity, five participants also referred to the uniqueness of the fingerprint data or the fact that it can identify the individuals (having these traits could make personal data very sensitive). However, other fingerprint characteristics such as availability everywhere and its unknown threats for our participants obviously outweighed its uniqueness and the fact that it can identify people and made those five participants to rate the sensitivity low. Users think security should be achieved by obscurity [1]. Pin codes are hidden but fingerprints are not.

¹⁴It is true if there is not a fingerprint pattern database to search in.

¹⁵For example, our age, gender, educational background, or our interests can be derived from an aggregated set of personal and behavioral data about us (i.e. derived/extracted data).

On the other hand, 78 participants rated sensitivity of fingerprint information 6 or higher (max. = 10). The most common reasons derived from their answers were the uniqueness of fingerprint information and the fact that fingerprint information can identify the person. Being unchangeable, possibility to be forged, copied, or replicated, being a part of the body and biological data, being used to authenticate and give access to other personal information and being used to identify the person in sensitive contexts were among the common reasons participants reported. Among people who rated the fingerprint information 6 for its sensitivity, some provided some reasons why they think it should be 6 and not more sensitive (i.e. somehow justifying why they did not rate it higher):

- Although it is unchangeable it is hard to forge/replicate/copy it.
- Although unique but if someone really wants it, can access it (like passwords).
- Although sensitive, the pattern alone may not be used practically in a very bad way, when it is in its digital form secured.

Finally, we consider all the people who reported that fingerprint pattern is very sensitive (a rate above 6) and as the reason, they mentioned that fingerprint can be forged/replicate/misused. Then we compare their answers to the question asking about the security of fingerprint vs. other measures (Q2 in Table 1). It turns out that among all of those ten participants, just two of them rated the security very low (i.e. rated it 1 and 2) and all others rated it 6 or above. It shows that although they think that the fingerprint pattern is sensitive because it may be forged/misused/replicated and used to impersonate them, fingerprint authentication still appears to them much more secure than other authentication measures like passwords.

7 CONCLUSION: IMPLICATIONS FOR FURTHER STUDIES

Several of the results from this study have methodological implications while others are more specifically related to the subject matter of user perception of authentication methods, in particular as regards fingerprint pattern usage. In all, nine points have been brought up in the previous sections based on quantitative or qualitative analysis of the respondents' answers. We highlight them here in the order they appeared in the results discussions.

Mockups can be profitably used. That is, simplified UIs in user studies that are not meant to measure the exact characteristics of fingerprint sensors, constitute a satisfactory proxy for using fingerprint sensors on mobile devices.

Knowledge in Computer Security seems to have a leveling effect on the real-life experience. Trust in a certain service provider does not influence the mental model of authentication procedures for people with some knowledge in IT security.

However, **self-estimation of knowledge in Computer Security is not a good predictor for the level of understanding of how authentication with different tokens is made on mobile devices.** In retrospect, our attempt to control whether the respondents were comparable to the respondents in [15] showed that we did not manage to keep outside computer science circles but on the other hand, we observed that claimed knowledge in Computer Security is not a good representative of individuals' understanding

of what entities have access to the authentication tokens. From this study, it seems arguable to recommend researchers to use control questions like our own on access to authentication tokens.

Current processes do not affect (and thus do not help) smartphone users to better understand. As reported by Zirjawi et al. [24], the most preferred combination of authentication systems seems to be fingerprint and password authentication. There are some studies showing that the potential of fingerprint method to provide additional security is not exploited by users. Wimberly and Liebrock [22] investigate if adding visible security features to a system causes users to reduce how much effort they make in other security areas. Wimberly and Liebrock's results demonstrate a strong correlation between greater faith in the perception of security for fingerprint-secured accounts and decreased password strength. Cherapau et al. [5] also present an investigation of the impact of Touch ID on passcodes used for unlocking iPhones. The results of user studies conducted by Cherapau et al. do not reveal any correlation between the use of Touch ID and the strength of users' passcodes. Overall, Touch ID users use weak unlocking secrets similarly to those users who do not use Touch ID [5]. Both studies corroborate the conclusion that current processes do not help users to understand the issues involved in authentication.

Non-users of fingerprint authentication tend to be more afraid of third-party access than users are. This result may not be surprising - at first sight, it may be explained by why people at all start to use the fingerprint sensor on their devices. However, out of 44 non-users 27 simply did not have such a sensor on their mobile.

Users of fingerprint authentication tend to regard fingerprint pattern as more sensitive than non-users do. This, in contrast to the previous point, might seem intuitively wrong. However, as pointed out before, there is no contradiction between the use of fingerprint sensor and a belief that fingerprint pattern may be sensitive information because as a token used for authentication this pattern is of course "sensitive".

People who connect a low degree of sensitivity to fingerprint patterns can have very different grounds for this judgment. This prompts us to call for more research as it is unclear if the different groups would benefit from different information to understand when the fingerprint is a secure or risky option. Are they repelled by information meant for the others? Can a UI be designed to cater to them both?

People do not seem to believe that other information besides identity can be derived from a fingerprint pattern. Thus, reports like [16] and [8] have probably not affected opinions of the general public.

Many people believe fingerprint patterns are sensitive information, at least to some degree. Some previous works also showed that users perceive that using fingerprint sensor on devices is more secure than other smartphone authentication mechanisms (see Section 6). However, these studies did not investigate what users think about problems and attacks for fingerprint vs. other measures. They just asked about the subjective opinion of users and the feasibility of bypassing fingerprint sensors. How more transparency of the mechanism involved for storing and processing fingerprint patterns on today's mobile devices for different purposes will affect people's perception about fingerprint sensitivity,

privacy, and security and their corresponding behaviours is an open question. For example, having access to a fingerprint template will not help to derive and make the original fingerprint pattern. Neither will copying fingerprint data from a different user on the same device or from another device work. These facts are explained in [21][2]. How can these facts be communicated effectively to users? And what would the impact on their perceptions and behaviours be?

ACKNOWLEDGMENTS

This research has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No.: 653454. Furthermore, the authors are grateful for the help from project assistant Daniel Lindegren who produced the videos and valuable comments from Dr. Charlotte Bäckman on the structure of the study.

REFERENCES

- [1] Ruba Abu-Salma, M. Angela Sasse, Joseph Bonneau, Anastasia Danilova, Alena Naiakshina, and Matthew Smith. 2017. Obstacles to the adoption of secure communication tools. In *2017 IEEE Symposium on Security and Privacy (SP)*. IEEE, 137–153.
- [2] Apple. 2018. iOS security, iOS 11. https://www.apple.com/business/docs/iOS_Security_Guide.pdf. (January 2018). Accessed April 23, 2018.
- [3] T Mark Beasley and Randall E Schumacker. 1995. Multiple regression approach to analyzing contingency tables: Post hoc and planned comparison procedures. *The Journal of Experimental Education* 64, 1 (1995), 79–93.
- [4] Rasekhar Bhagavatula, Blase Ur, Kevin Iacovino, Su Mon Kywe, Lorrie Faith Cranor, and Marios Savvides. 2015. Biometric authentication on iPhone and Android: Usability, perceptions, and influences on adoption. In *Proc. USEC'15*. Internet Society, 1–10.
- [5] Ivan Cherapau, Ildar Muslukhov, Nalin Asanka, and Konstantin Beznosov. 2015. On the impact of Touch ID on iPhone passcodes. In *SOUPS 2015*. USENIX Association, 257–276.
- [6] Alexander De Luca, Alina Hang, Emanuel Von Zezschwitz, and Heinrich Hussmann. 2015. I feel like I'm taking selfies all day!: towards understanding biometric authentication on smartphones. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. ACM, 1411–1414.
- [7] Miguel A Garcia-Perez and Vicente Nunez-Anton. 2003. Cellwise residual analysis in two-way contingency tables. *Educational and psychological measurement* 63, 5 (2003), 825–839.
- [8] Richard Green and Robert Young. 2000. Fingerprint asymmetry in male and female transsexuals. *Personality and Individual Differences* 29, 5 (2000), 933–942.
- [9] Marian Harbach, Alexander De Luca, and Serge Egelman. 2016. The anatomy of smartphone unlocking: A field study of android lock screens. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. ACM, 4806–4817.
- [10] Marian Harbach, Alexander De Luca, Nathan Malkin, and Serge Egelman. 2016. Keep on lockin' in the free world: A multi-national comparison of smartphone locking. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. ACM, 4823–4827.
- [11] Edward Higgs. 2010. Fingerprints and citizenship: the British state and the identification of pensioners in the interwar period. In *History Workshop Journal*, Vol. 69. Oxford University Press, 52–67.
- [12] Felix Hörandner, Stephan Krenn, Andrea Migliavacca, Florian Thiemer, and Bernd Zwattendorfer. 2016. CREDENTIAL: a framework for privacy-preserving cloud-based data sharing. In *Availability, Reliability and Security (ARES), 2016 11th International Conference on*. IEEE, 742–749.
- [13] Crystal Huynh, Erica Brunelle, Lenka Halámková, Juliana Agudelo, and Jan Halámek. 2015. Forensic identification of gender from fingerprints. *Analytical chemistry* 87, 22 (2015), 11531–11536.
- [14] Younsa Javed, Mohamed Shehab, and Emmanuel Bello-Ogunu. 2017. Investigating user comprehension and risk perception of Apple's Touch ID technology. In *Proceedings of the 12th International Conference on Availability, Reliability and Security*. ACM, 35.
- [15] Farzaneh Karegar, Daniel Lindegren, John Sören Pettersson, and Simone Fischer-Hübner. 2018. User evaluations of an app interface for cloud-based identity management. In *Advances in Information Systems Development*, Nearchos Paspallis, Marios Raptopoulos, Chris Barry, Michael Lang, Henry Linger, and Christoph Schneider (Eds.). Springer, 205–223.
- [16] Doreen Kimura and Michael W Carson. 1995. Dermatoglyphic asymmetry: Relation to sex, handedness and cognitive pattern. *Personality and Individual Differences* 19, 4 (1995), 471–478.
- [17] Els J Kindt. 2009. The use of privacy enhancing technologies for biometric systems analysed from a legal perspective. In *IFIP PrimeLife International Summer School on Privacy and Identity Management for Life*. Springer, 134–145.
- [18] Els J. Kindt. 2013. *Biometric data, data protection and the right to privacy*. Springer Netherlands, Dordrecht, 87–272. DOI: http://dx.doi.org/10.1007/978-94-007-7522-0_3
- [19] Alina Krupp, Christian Rathgeb, and Christoph Busch. 2013. Social acceptance of biometric technologies in Germany: A survey. In *Biometrics Special Interest Group (BIOSIG), 2013 International Conference of the*. IEEE, 1–5.
- [20] Andreas Pfitzmann. 2008. Biometrics—how to put to use and how not at all?. In *International Conference on Trust, Privacy and Security in Digital Business*. Springer, 1–7.
- [21] Android Open Source Project. 2018. Android Security. <https://source.android.com/security/>. (March 2018). Accessed April 23, 2018.
- [22] Hugh Wimberly and Lorie M Liebrock. 2011. Using fingerprint authentication to reduce system security: An empirical study. In *Security and Privacy (SP), 2011 IEEE Symposium on*. IEEE, 32–46.
- [23] Verena Zimmermann and Nina Gerber. 2017. "If it wasn't secure, they would not use it in the movies"—Security perceptions and user acceptance of authentication technologies. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*. Springer, 265–283.
- [24] Nedaa Zirjawi, Zijad Kurtanovic, and Walid Maalej. 2015. A survey about user requirements for biometric authentication on smartphones. In *Evolving Security and Privacy Requirements Engineering (ESPRE), 2015 IEEE 2nd Workshop on*. IEEE, 1–6.