I Feel Like I'm Taking Selfies All Day! Towards Understanding Biometric Authentication on Smartphones

Alexander De Luca[1,2], **Alina Hang**[1], **Emanuel von Zezschwitz**[1], **Heinrich Hussmann**[1]
[1]Media Informatics Group, University of Munich (LMU), Munich, Germany
[2]DFKI GmbH, Saarbrücken, Germany
{alexander.de.luca, alina.hang, emanuel.von.zezschwitz, hussmann}@ifi.lmu.de

ABSTRACT
We present the results of an MTurk survey ($n = 383$) on the reasons for using and not using biometric authentication systems on smartphones. We focused on Apple's Touch ID as well as Android's Face Unlock as they are the most prevalent systems on the market. For both systems, we categorized the participants as a) current users, b) former users that deactivated it at some point and c) nonusers. The results show that usability is one of the main factors that influences the decision on whether or not to use biometric verification on the smartphone. To our surprise and as opposed to previous research on biometric authentication, privacy and trust issues were not among the most important decision factors.

Author Keywords
Biometric authentication; Face Unlock; Touch ID

ACM Classification Keywords
H.5.m. Information Interfaces and Presentation (e.g. HCI): Miscellaneous

INTRODUCTION
Biometric authentication is often referred to as the secret weapon of authentication, mainly due to the fact that the "password" (e.g. a fingerprint) cannot be forgotten [3]. This might be one of the reasons why many smartphone companies and operating system developers recently started integrating biometric authentication into their systems. The two most prominent examples are Face Unlock (introduced with Android 4.0) and Touch ID (a fingerprint scanner that was introduced with Apple's iPhone 5s). These two systems represent the first noteworthy deployment of biometric authentication in end consumer mobile devices. From a user-centered point of view, this raises a lot of interesting questions.

Despite its advantages, privacy and security issues are often mentioned as one of the main reasons or even the most important factors for a user's decision to avoid using biometric authentication in general [3]. In addition, many biometric approaches, like speaker recognition, are considered insecure by their users [7]. Recently, Chandrasekhar et al. [2] explored the usability of Touch ID and Face Unlock in a lab study and found that external factors like awkwardness when holding the device in front of the face to perform an unlock had a great negative influence on the perceived usability of the systems and the participants' willingness to use them.

In this work, we were interested in factors that cannot be evaluated in a lab study. Therefore, we performed an MTurk survey with 383 participants that own devices capable of either Face Unlock or Touch ID. We focused on the reasons that make people (not) use the biometric authentication functionalities on their own smartphones. For each authentication system we divided the results into three categories: a) activated, i.e. people that activated the system at some point and are still using it; b) deactivated, i.e. people that used the respective system but stopped using it; c) never activated, i.e. people that never activated the feature on their devices.

The main contribution of this paper consists in focused insights into reasons for using or not using biometric authentication on smartphones. We identify the main factors that influence this decision. For instance, as opposed to previous work, privacy issues were not among the main reasons for not using biometric authentication. Other factors like usability and reliability were considered much more important. These insights can help to design the systems in a way that increases user acceptance of biometric authentication on smartphones.

SURVEY
We conducted an online survey using Amazon's Mechanical Turk (MTurk) service. Even though MTurk has its limitations, MTurk studies can create meaningful and valuable results in the area of usable security if adequate measures to secure response quality are taken (e.g. control questions).

SURVEY DESIGN
As mentioned before, we decided to limit the study to Android's Face Unlock and Apple's Touch ID as they represented the most common systems at the time of this study. Therefore, we created two different MTurk tasks. The study was advertised on MTurk as being about biometric systems and Android's Face Unlock or Apple's Touch ID respectively. Workers that wanted to participate in the survey had to be US residents and needed a HIT/task approval rate (approved correct participation in previous MTurk tasks) of 90% or higher. Furthermore, the study description mentioned that they had to own a compatible device (e.g. an iPhone 5s for Touch ID).

CHI 2015, April 18–23, 2015, Seoul, Republic of Korea.

ACM 978-1-4503-3145-6/15/04...$15.00.
http://dx.doi.org/10.1145/2702123.2702141

	Touch ID			Face Unlock		
	M/F	Age	%	M/F	Age	%
activated	82/76	27 (18-47)	86.3	6/12	30 (20-51)	10
deact.	10/7	29 (20-42)	9.3	44/34	28 (18-61)	38.5
never act.	1/7	26 (20-37)	4.4	55/49	29 (18-58)	51.5
overall	93/90	27 (18-47)		105/95	28 (18-61)	

Table 1. Survey demographics and percentage of participants that have the respective system activated, deactivated it or never activated it.

The two tasks led to two different surveys hosted on our servers. The surveys were identical with the exception of the authentication mechanism they focused on. They started with a description of the respective system followed by a section about demographics. After that, the participants were asked whether they are using the respective system, have been using it or never tried it. Depending on the answer, the remainder of the survey focused on this specific context. For instance, nonusers were asked "*Why do you not use [system]?*" while participants that had used the system before and then deactivated it were asked two questions instead: "*Why did you use [system]?*" and "*Why did you stop using [system]?*".

To make sure that the participants fulfilled the requirements of the study, the survey contained control questions as well as a simple task in which the participants were asked to submit a photo of their smartphone recorded with the device itself using the front camera and a mirror. The questions as well as the photo were manually checked before approving the respective participant. Afterwards, the photos were deleted.

On average, the survey took around 20 minutes. Approved Turkers received US$ 1 for their effort, which is a common compensation for such tasks on MTurk.

Participants

The Face Unlock survey was active for 15 days until 200 submissions were approved (20 rejected). The Touch ID task was stopped after 33 days and 183 submissions were approved (28 rejected). Table 1 shows the participants' demographics.

RESULTS

For the analysis, all open-ended questions were coded using an inductive approach. Two researchers independently created codes and then met to create the final codeplan. This was then used by a third and fourth researcher to do the final coding of the responses. In all instances, saturation points of new themes were reached before the final data were coded (e.g. after 10 out of 17 participants that deactivated Touch ID). We therefore argue that our results cover the most relevant reasons for (not) using biometric authentication on smartphones.

Categories

Table 1 lists the percentage of participants that either had the respective system activated, had never activated it or had deactivated it after some time. The data reveals three noticeable trends: 1. The number of active Touch ID users is much higher than in any other category. 2. With 52%, the amount of participants that never activated Face Unlock on their devices is very high. 3. Considering the fact that the number of active users plus the number of former users represents all participants that ever used the respective system, this means that Face Unlock has a very high dropout rate of 81.3%. On the other hand, the dropout rate for Touch ID is only 9.7%.

Active Users

The results of the coding of reasons for using Face Unlock and Touch ID are listed in table 2. The main reason for using Touch ID as named by the participants is usability. Examples include speed and convenience of authentication. Many participants named it to be as easy and fast as the normal slide to unlock. Please note that reliability can be considered an important factor of usability but is listed independently in the table. For Face Unlock, usability only plays a minor role with security being the most important reason of use.

Emotion is also considered an important factor in the decision to use Touch ID. For instance, participants called it "*fun*", "*interesting*", "*joyful*" and even "*awesome*". Such positive emotional aspects were only mentioned once for Face Unlock.

In the survey, participants were also asked which authentication mechanisms they used on their smartphones before activating the respective biometric system. To gain insights into whether providing biometric authentication has a potential impact on secure behavior, we analyzed how many of them had not used an authentication mechanism before on their smartphone. For Touch ID, 24 out of 158 participants (15%) decided to use authentication due to the availability of the biometric technology. For Face Unlock, 4 out of 20 participants (20%) made this decision.

Former Users

Participants that deactivated Face Unlock or Touch ID made the decision to use the respective system at some point but then got rid of it. The reasons for this decision reveal how and why biometric systems can disappoint their users. The reasons are outlined in table 2. Even though the dropout rates for Touch ID are very low and thus the numbers have to be interpreted carefully, usability together with reliability seem to play an important role in the decision process. For Face Unlock, with 28 (36%) participants, this trend is clear and was in many instances coupled with emotional aspects like annoyance.

The main usability problems for both systems were slow speed and lack of convenience. For instance, participants that stopped using Face Unlock thought it was way too slow especially in cases when they needed quick access to their devices. In addition, correctly aligning the device in front of the face was considered unnecessarily difficult.

External factors were mentioned by 23 (29%) participants as being an important factor to stop using Face Unlock. Besides bad lighting conditions leading to bad performance, the participants mentioned social awkwardness as an important external factor that kept them from using the system. The two instances for Touch ID were due to the participant's work which negatively influenced the performance of Touch ID (e.g. oily hands) and using a protective phone case which made using the system impossible.

	Touch ID		Face Unlock	
	reason	count	reason	count
activated	Usability	110 (70%)	Security	8 (44%)
	Security	61 (39%)	Curiosity	4 (22%)
	Emotion	20 (13%)	Usability	3 (17%)
	Privacy	6 (4%)	Novelty	1 (6%)
	Novelty	6 (4%)	Emotion	1 (6%)
	Reliability	6 (4%)	Prestige	1 (6%)
			Reliability	1 (6%)
deactivated	Usability	8 (47%)	Usability	28 (36%)
	Emotion	3 (18%)	Reliability	23 (29%)
	Reliability	3 (18%)	External Factors	23 (29%)
	External Factors	2 (12%)	Emotion	12 (15%)
	Security	2 (12%)	Security	11 (14%)
			No Need	5 (6%)
			Technical Misconception	1 (1%)
never activated	Usability	3 (38%)	Ignorance	28 (27%)
	Technical Misconception	3 (38%)	No Need	24 (23%)
			Reliability	24 (23%)
	Trust	2 (25%)	Usability	23 (22%)
	Reliability	1 (13%)	Emotion	15 (14%)
	External Factors	1 (13%)	Security	8 (8%)
			Technical Misconception	7 (7%)
			External Factors	4 (4%)

Table 2. Reasons for using, not using and deactivating Touch ID and Face Unlock. Please note that participants' answers can relate to several of these categories and thus do not add up to 100%.

We also asked participants about what changes to the system would be required to make them use it again. The most important factor was usability together with reliability, which was mentioned by 36 (46%) Face Unlock and 9 (53%) Touch ID participants. Security improvements were mentioned by 29 (37%) Face Unlock participants, but were not mentioned at all in the Touch ID group.

Nonusers

The main reasons for participants that never activated the systems are listed in table 2. The results show that a high number of participants (27%) that never used Face Unlock on their devices, simply did not know that it existed (coded as "Ignorance" in the table). This number is zero for Touch ID users. Assumed reliability and usability problems as well as the group of participants that thought that their current level of protection was enough represent important factors as well.

In the small Touch ID group, technical misconception was one of the main reasons for nonuse. For instance, two participants stated that their device was used by at least one additional person. They were convinced that sharing their device would not be possible anymore once Touch ID was activated (which is not correct as the system allows to store several fingerprints). Furthermore, the only two instances of participants that did not use the system due to trust and privacy issues can be found in this group. These participants stated that they did not trust the respective company with their fingerprint data.

DISCUSSION

Usability Top Argument

In all conditions, usability was one of the top factors that influenced the decision to use or not use the respective system. Touch ID was considered as more usable than the alternatives (e.g. PIN) which made it a very convenient and useful option for the participants (even first time adopters). It seems to be better integrated into the interaction process and does not add much overhead (or even none) to the overall unlocking process. In many cases, it was considered equally fast and easy as slide to unlock. The bad usability and reliability properties of Face Unlock seem to explain the high dropout rates much more than any other factor. Please note that external factors do contribute to the usability rating as they were the reason for interaction problems in many cases.

Harbach et al. [6] recently performed a real world study on smartphone unlocking and found that users spend a significant amount of the overall device usage time on entering their PINs or unlock patterns. In most cases, securing the device was not even necessary. This explains how the increased error rate and the reduced authentication speed of Face Unlock as reported by the participants highly influence the decision to deactivate the system. It also highlights the fact that authentication systems (biometric or not) that do not provide high usability properties are not appropriate for standard authentication on smartphones.

Role of Privacy and Trust

When discussing biometric authentication from a user's point-of-view, privacy and trust are often mentioned as being one of the main reasons for not using a biometric system [3]. Users are cited as being highly critical about how their data is used and where it is stored. To our surprise, privacy and trust were only mentioned by two participants. They stated that they never activated Touch ID as they were afraid of what the smartphone and the respective company would do with their data.

Our data does not allow to fully investigate this issue but we believe that this is due to a couple of reasons. Our main hypothesis is that it can be partially attributed to the fact that smartphones are considered very private devices by their owners. This is supported by the fact that 93 (59%) of the 158 Touch ID users explicitly stated to believe that their fingerprint data is only stored locally on their device.

System developers should embrace this trust by building systems that behave this way. In addition, they should communicate transparently to their users what happens to their data.

Technical Misconception

Even though technical misconceptions were mentioned only in a few instances, they are one of the two top reasons in the (small) group of Touch ID device owners that never activated the fingerprint scanner. The interesting part is that this category represents reasons that are factually wrong but still lead the respective participant to not using a potentially helpful and useful feature. Such misconceptions should be avoided through appropriate communication and also at the interface level, for instance during the setup phase.

First Time Adopters

The analysis of the data revealed a very interesting trend. A certain number of participants (Touch ID: 15%; Face Unlock: 20%) that actively use the systems only decided to turn on authentication due to the availability of a biometric system. On their previous devices and before using Touch ID or Face Unlock, they did not use any other form of protecting their data through authentication. Please note that all of them had smartphones before they started using their current devices.

We therefore argue that the availability of a well-designed biometric authentication system can have a positive effect on the protection of the users' smartphone data. This was recently also observed by Egelman et al. [4] who reported on a study participant that only used authentication due to the convenience level provided by Touch ID.

Social Compatibility

Many external factors that made participants stop using Face Unlock were related to awkwardness when using the system in public. For instance, participants said that holding the device in front of their face made them feel weird. One user stated that "*It can be a bit embarrassing to hold your phone up in a weird position while in public just to unlock it.*". Another user noted that she would not use Face Unlock as it "*looks like I'm taking selfies all day.*". For Touch ID, no such complaints were raised.

Our results thus support the claims by Hang et al. [5] who found that social awkwardness was one of the major reasons why users in a big company were not satisfied with using their internal voice recognition system. This seems to apply even more to the smartphone context as much of the interaction with these devices takes place in public.

Advertising

Our data suggests that advertising had a big effect on the decision to activate Touch ID which was heavily advertised through all media. The lack of knowledge about the availability of Face Unlock on their devices (27% of nonusers) can be partially explained due to the fact that, with the exception of specialized media (e.g. computer magazines), this feature was not publicized at the time of our study. The importance of this is highlighted by the fact that the 8% of nonusers that mentioned security problems for not using Face Unlock were not aware of current security improvements to the system like "Wink to Unlock" which requires the user to wink to prove that the camera is not recording a static image.

Sense of Security

Even though the participants did, in many cases, not fully understand the technology of the specific system and even though they were not aware of current developments and improvements to Face Unlock, they were surprisingly good in estimating their relative security improvement/loss. For instance, all Face Unlock users were aware of the fact that it could potentially be spoofed with a photo of the user [1]. This indicates that, with respect to security, users make informed decisions and giving up security (e.g. for usability) often happens voluntarily.

CONCLUSION AND LIMITATIONS

Our survey provides first insights into the decision making process of the use of biometric authentication mechanisms on smartphones. Among others, our results show that, as opposed to previous work, trust and privacy issues are not major factors while usability is one of the top arguments for (not) using the systems. Furthermore, we provide recommendations such as considering the importance of "social compatibility" when developing biometric authentication systems for use on smartphones and thus potential public use.

Even though our study provides interesting insights into the topic, there are a few limitations that have to be considered carefully. For instance, the numbers of participants in some categories (e.g. Touch ID deactivations) is quite low. In addition, all study participants were US residents. This limits generalizability of the results. In future work, the study should be repeated with other populations to see if the results hold true for these as well.

Furthermore, at the time of the study, Face Unlock was significantly longer available than Touch ID. However, the results of the questionnaire indicate that most participants just recently started using both features with almost no early adopters in the Face Unlock group. Still, we cannot state with 100% certainty that this difference had no influence on the results. The study should be repeated in the next years to compare the results to our current insights.

REFERENCES

1. Anjos, A., and Marcel, S. Counter-measures to photo attacks in face recognition: A public database and a baseline. In *Proc. IJCB '11*, IEEE (2011), 1–7.
2. Bhagavatula, C., Iacovino, K., Kywe, S. M., Cranor, L. F., and Ur, B. Poster: Usability analysis of biometric authentication systems on mobile phones. *SOUPS Poster* (2014).
3. Coventry, L., De Angeli, A., and Johnson, G. Usability and biometric verification at the atm interface. In *Proc. CHI '03*, ACM (2003), 153–160.
4. Egelman, S., Jain, S., Portnoff, R. S., Liao, K., Consolvo, S., and Wagner, D. Are you ready to lock? understanding user motivations for smartphone locking behaviors. In *Proc. CCS '14*, ACM (2014), 750–761.
5. Hang, A., De Luca, A., Frison, K., von Zezschwitz, E., Tedesco, M., Kockmann, M., and Hussmann, H. Travel routes or geography facts? an evaluation of voice authentication user interfaces. In *Proc. INTERACT '13*, Springer (2013), 468–475.
6. Harbach, M., von Zezschwitz, E., Fichtner, A., De Luca, A., and Smith, M. It's a hard lock life: A field study of smartphone (un)locking behavior and risk perception. In *Proc. SOUPS '14*, USENIX Association (July 2014), 213–230.
7. Sieger, H., Kirschnick, N., and Möller, S. Poster: User preferences for biometric authentication methods and graded security on mobile phones. *SOUPS Poster* (2010).