Bachelor Thesis
Computing Science

Radboud University

User understanding and user acceptance of biometric authentication on mobile phones

Author:

Leon vd Boogaard
s590058

First supervisor/assessor:

Dr. Eelco Herder
eelcoherder@cs.ru.nl

Second assessor:

Dr. Hanna Schraffenberger
h.schraffenberger@ru.nl

March 21st, 2022

Abstract

The aim of this thesis is to gain an insight about how users understand and accept biometric authentication options on their mobile devices, for various online services. Nowadays almost everybody possesses a smartphone with the capability of reading certain biometric traits such as fingerprints or a facial structure. This has opened ways to quickly unlock your device using this fingerprint but has not stopped there. Other applications can also use this fingerprint sensor. In the future the use of biometrics is believed to increase even further. But how good is the understanding of the everyday user of this 'new' technology? In this study we look into the process and motivations persons could have to eventually use biometric authentication options. This is done by first highlighting the possibilities, advantages and disadvantages and what can be done according to the law. Then we look at the beliefs of persons in earlier studies and related work and find some common misconceptions about the use of biometric authentication. Based on all these factors we conduct a study using a questionnaire to gain further understanding about the motivations users could have for their decision to use biometric authentication.

Content

1. Introduction

We all have a smartphone in our pockets and the number of applications and things to do on them is ever growing. Most applications or online services being used requires their own way for the user to log in or authenticate themselves. This results in an increasing number of accounts, passwords and other ways to log in.

Almost all mobile devices being shipped nowadays also give users the option to unlock them using their biometrics, for instance fingerprints or by scanning the face. Biometric authentication has become more advanced and widely accepted. We basically all have a biometric reader in our pockets on a daily basis. This can be a fingerprint sensor or the camera that captures your face when you unlock your phone.

With this increase of times and ways to authenticate yourself to some application or online service on your own mobile device, biometrics are being more accessible and a normal way to do this. Instead of having to remember a password for every online account you use you can just log in using your fingerprint.

Several applications offer the option to replace the more conventional combination of username and password with a form of biometric authentication. Some examples are online banking applications, which allow you to authenticate yourself with your fingerprint or face scan instead of your pin code. WhatsApp offers the option to further secure your personal data by adding an extra layer of security in the form of biometrics.

This rising trend in usage and acceptance of our daily use of biometrics on our mobile devices can raise some questions. On one side biometrics are a really powerful way to identify a person, but the sensitive nature of the biometric data raises some concerns about privacy and intrusion. One could ask themselves what the next application is that wants to use biometric authentication and whether users are ready for that.

Some applications and services that might be interested in using biometrics in the future are for instance online streaming platforms. In this day and age almost everybody uses one, if not more, of them. Examples are Netflix, Amazon Prime, Disney+ or Videoland. It is not a secret that many people share an account for these services to reduce cost or because it is easier. But the big companies behind these services would rather not have you do this since this reduces profits.

Over the years attempts to make this account sharing harder have already been implemented. Some services require you to log in more often when for instance the IP-addresses are out of order. Other examples are the use of two-factor authentication, to make it annoying for people to share their password. But can they go even further than that? What if these streaming services require a user to authenticate themselves using biometrics every time they want to watch a movie? This will make account sharing even harder and therefore possibly increase the profits of these big corporations.

In 2017, the Alliance for Creativity and Entertainment (ACE)[1] was founded. This is a coalition between almost all big corporations in the media landscape, such as Netflix, Amazon, HBO, Sony, Star and Warner Bros. Their goal is to end illegal acts of digital piracy, which includes the illegitimate sharing

[1] Alliance for Creativity and Entertainment, https://www.alliance4creativity.com/

of accounts. This has sparked the discussion[23] on what draconic measures these services are willing to take, such as using biometrics in order to stop users from sharing their passwords.

In this thesis I want to look into the user acceptance of using biometric authentication schemes on different applications or services. This raises the following research question:

"What is the attitude of users towards biometric authentication for different types of online services?"

We will answer this question by first looking at how biometric authentication works and what its general advantages and disadvantages are. We also give a short insight about how this is all regulated by law and how it works on smartphones. Next, we look at known works that give an indication on how users may perceive the usage of biometric authentication. This is done in section 2. Then we will conduct a study to further understand users' behaviour in which the methodology will be explained in section 3 and its results shown in section 4. In section 5 we will give an interpretation and discussion of the results.

[2] Biometric Big Brother: Streaming Services Want Thumbprint Verification for Access, November 11th, 2019, https://www.extremetech.com/internet/301724-biometric-big-brother-streaming-services-want-thumbprint-verification-for-access

[3] Netflix and other streaming platforms are considering fingerprint check, November 28th, 2019, https://iics.medium.com/netflix-and-other-streaming-platforms-are-considering-fingerprint-check-44bb7588f9f1

2. Background

2.1 Biometric Authentication

In our modern (online) society, authentication and verification of persons has become more important. Whether it is for travel, doing official paperwork or other buying a beer when you look a bit young, everybody nowadays is required to be able to identify themselves. We all have a passport, ID card or drivers' licence to show authorities who we are. But it does not stop with only these official documents. Many employees or students have some sort of card or identification badge to prove that they belong to a certain organisation. These can be used in the process of *authentication*, e.g., to see if somebody is who he claims he is.

With the increase of technological advancement, new ways to authenticate yourself have become more relevant and easier, in particular the use of biometrics. Biometrics are biological or physical characteristics that define and identify an individual. These characteristics can be physical, such as fingerprints or the way your face is structured, but also behavioural, such as the way people walk or type. We see that biometrics are being used more regular over the past years. Since 2004, the European Union requires every passport being issued to have biometric data in the form of a facial image and fingerprint on them (Habibu et al., 2019). This makes identifying persons easier, for instance at the customs when traveling. But also, in everyday use biometric authentication has become more available. Almost all new smartphones offer biometric authentication of some sort, with Android relying on the fingerprint scanner and Apple's FaceID on iPhones. A lot of smartphone users use these functions because it is faster, easy and secure.

2.2. Advantages and disadvantages of using biometric authentication

The usage of biometrics for the purpose of authentication or identification has been around for quite some time now. There have been several researches on its usage and the different types (Alsaadi, 2015) of implementation. The study of (Matyás & Ríha, 2002) began in 1999 and looked at the possibilities of biometrics in general and its advantages and disadvantages. Because the capability of technology and devices has increased exponentially since then, there are even more things to be said about biometrics in general. In this section I will provide a general overview about the main advantages and disadvantages that different biometric authentication systems could have and provide possible solutions to these disadvantages.

2.2.1 Advantages

There are several big advantages that biometric authentication has over the more general authentication schemes such as a password or PIN-code. One of the most obvious ones is that you always have your biometrics 'on you'. A password can easily be forgotten, but your biometric features are *always present*. This means users will have to rely less on *what they know*, but instead *what they are*. This can result in much easier use of different authentication systems, such as fingerprint scanners or facial recognition cameras(Meng et al., 2015).

When the technical implementation of the biometric authentication scheme is done in a proper way, they can be the strongest form of authentication there is. Some biometric traits are *unique* and differ for everybody, like fingerprints and iris structure(Wolf et al., 2018). These are unique to every human being and can therefore be used to directly link a biometric to a person. Because of the increasing quality of the technology behind biometric scanners, they have become almost impossible to fool.

For these unique biometric traits, authentication can be done in a way more secure and precise manner and can therefore help in telling if a person is really who they say they are.

Another advantage is that most biometric traits are *permanent and non-changeable*(Matyás & Ríha, 2002). This is a great asset for authentication. The user of a biometric authentication scheme will only need to provide their data once if done correctly. This also increases the overall strength of using biometrics over traditional authentication schemes.

Biometric characteristics can not be '*stolen*' or shared with others. This is a big advantage considering traditional authentication schemes where for instance a password is used. If a user is victim to a password hack or database breach, somebody else could authenticate themselves using their password(Peng et al., 2019). Another traditional way of authentication could be by the means of smartcards or other physical tokens. But these can also be stolen or intentionally misused. When using biometrics this simply is not possible.

In most cases biometric authentication systems are *easier* for users than conventional systems(Matyás & Ríha, 2002)(Byun & Byun, 2013). It takes little effort to have your fingerprint scanned or your picture recognized by computer systems. When authenticating with a password, users need to put in way more effort than simply providing the correct biometric sample.

Added to the ease of using biometric authentication systems, there is also a general advantage in *speed*. While it takes some time to enter your password, a fingerprint scan can be done instantly with nowadays technology. When looking at the way persons use smartphones in particular, it is faster and more convenient to unlock it with your fingerprint than with a PIN-code or pattern.

2.2.2 Disadvantages

There are also some disadvantages about using biometric authentication. When using physiological biometrics one drawback could be that people with *disabilities* might not be able to use them(Blanco-Gonzalo et al., 2018). Amputees could for instance be unable to provide their fingerprints. Other physical disabilities might limit the effectiveness of biometric authentication systems too. But because there are several different possible implementations of biometric authentication, the possibility to still be able to use one of your biometric traits is still very probable.

One concern about using biometrics for the means of authentication is that biometrics are *not secret*(Zirjawi et al., 2015). If you authenticate with your own password that you keep in your brain, no one will know it unless you share it with others. Your biometric traits are much less of a secret. Everybody can see your face and if you try really hard, your fingerprints. When using facial recognition technology, the camera could be spoofed with a picture of the person that is trying to authenticate, instead of the person itself. This could be prevented in the implementation of the system. In the case of a facial scan, it could simply be done to let the person blink or make sure a three-dimensional object is being scanned. This all depends on the way the actual authentication is being implemented.

Another possible disadvantage about biometric authentication is the *hardware*. When implementing some biometric authentication scheme, the hardware needs to be trusted and not easily be fooled. With fingerprint authentication a special device is needed to convert your fingerprint to a digital reading. This hardware needs to be of provable quality in order for users to actually trust it.

The main advantage to biometric authentication could also be seen as a disadvantage. Biometrics allow us to uniquely identify one particular person, but this also raises the question about *privacy* issues(Arora & Bhatia, 2021). Sharing your biometric traits such as fingerprints or face scan may feel

more intrusive than just picking a password for authentication. Biometric data contains a lot more information about a person than a password or PIN-code. When passwords get leaked, one could deal with the damage and pick another password. But a person can not change their fingerprints or face in case this data gets hacked into. In order to prevent this from happening, a lot of progress has been made in laws such as the GDPR to improve user privacy and protection.

Sometimes different *circumstances* don't allow biometric authentication to be used(Alsaadi, 2015). This has to do with the physical factors that are always present when using biometrics. If you have a small cut on your finger, a fingerprint sensor could for instance deny your authentication request, while you are the person you claim to be. Also, things like sweat or raindrops may lessen the workings of a fingerprint scanner. Other biometric sensors that rely on images such as iris scans or facial recognition technology could suffer from bad lighting. To circumvent these inconveniences, the system could offer an alternate way of authentication, besides the biometric option.

2.3 Biometrics and law

With technological innovations on the rise and becoming ever more important in everyday use, the need to regulate digital data has also become a bigger factor. Over the years many attempts have been made to enforce the proper handling of personal data in different laws, with each different country having their own rules. This has been an issue for quite some time, since the internet does not have any borders. In practice it is very hard to determine in what legislation some online and digital offences or abuses fall. This is why the European Union has been working on a new law that will hopefully make an end to this, at least for all EU citizens.

2.3.1 GDPR

This new law is called the General Data Protection Regulation, or short: GDPR(Data Protection Act, 2018). The GDPR has come into force from 28th of May 2018, and effects all EU citizens. The law is a new basis of how personal data should be processed and when it is legally possible to do so. It also aims to enhance users' privacy and data rights. Under the GDPR, three parties are considered. These are the *data subject, controller* and *processor*. The data subject is any EU citizen that has data collected about them by some organisation. The whole aim of the GDPR is to protect the data subjects(Gruschka et al., 2019). The data controller is the party that determines the purpose and the means of the data being processed. The data processor is the party that does the actual processing of the data. The processor and the controller can be the same party.

The term *processing* is very broad under the GDPR. Basically, anything that can happen to digital data concerning a data subject falls under the processing terms. This includes, among others, storing, analysing, altering and collecting data. The GDPR protects the data subjects' privacy and rights by imposing obligations to the data controller and by increasing the power of data subjects. This means that this law is big step forward in online privacy from a user's perspective.

One of the main goals of the GDPR is to limit the processing done by data controllers. This is enforced by a set of principles described in its article 5. In short, it brings strict rules regarding to the data collected and the purpose of the data processing. All these principles are there to make sure the processing of data is done in a correct way with as little as possible damage or privacy intrusion to the data subject. One other goal of the GDPR is to enhance the rights of the data subjects. This is done to improve transparency and give more control over your data.

The reason that earlier laws regarding online privacy and data protection failed is that every country had their own rules and the punishments for infringement were not severe enough. This is done

different with the GDPR. All member states are now obliged to implement this law, and the fines that come with any wrongdoing are made to be really high. There are two tiers of fines that a data controller could face when not respecting the GDPR. Either a fine of €10 million, or 2% annual global turnover, whichever is higher, or a fine of €20 million, or 4% annual global turnover, whichever is higher. The height of the fine will depend on what article is breached. These are huge amounts of money, with the idea that data controllers and processors are now extra aware to keep the privacy of data subjects more in mind.

2.3.2 Biometrics in the GDPR

In the GDPR there is a difference made between 'normal' data and certain special categories of personal data(Data Protection Act, 2018). These special categories consist of any personal data that are by nature more sensitive to the natural persons they represent. Some examples are data regarding ethnics, political opinion, health data, sexual orientation and biometrics. The processing of data that falls within any of these categories is prohibited by default, but there are some exceptions. Due to these exceptions in the law, the possibilities to use biometrics in daily authentication schemes is still possible. When the users give their consent, this is immediately allowed.

When using biometric authentication on your smartphone, the biometric data never leaves your device(Stokkenes et al., 2018). If this would be the case and for instance your smartphone's manufacturer would receive your fingerprint, they would have to comply with all these rules set up in the GDPR which is nearly impossible[4]. This means that every time you scan your fingerprint for instance, you are the data controller since you own your smartphone.

2.4. How do biometrics work on a smartphone?

To understand the user behaviour regarding biometrics on their smartphones, we have to take a deeper look into what is actually happening inside their devices. When using biometric authentication options on your smartphone, at one point you had to perform a certain number of steps in order to use it.

If you want to use your fingerprint on your device, you have to add it. This is done in the enrolment stage. The operating system will instruct the user to place his desired finger on the sensor a couple of times, until it has got an extraction of your fingerprints. The sensor looks at the directions of the grooves in the skin and uses that to generate a digital representation of your fingerprint. Then it is added to the local database on your device for future use.

The storage of your fingerprint and with that your biometric data is done exclusively on the device itself and will never leave it. The way it is stored is even more secure(Android Documentation, 2020). All biometric data are stored on a separate part of the device's storage and only limited functions have access to this part of your storage. This means that no third-party application or file manager can easily access your raw biometric data.

When using the fingerprint to unlock your device or authenticate yourself in any other application, certain APIs are called that run in their own protected environment, which increase the security even further. The user again places their finger on the sensor which creates a new, temporary reading of your fingerprint. Then it is tried to be matched with already stored fingerprints and if there is a

[4] Using biometric data? Sensitive under the GDPR!, October 18th, 2017, https://www.ictrecht.nl/en/blog/using-biometric-data-sensitive-under-the-gdpr

match, you are authenticated. This all happens in a split second which makes it much faster than having to enter a pin code, pattern or password.

2.5. Why are users (un)willing to use biometric authentication

With the increasing possibilities that technology offers nowadays, biometric authentication schemes have become more widespread among different fields and usages. But the sensitive nature that is incorporated with biometrics brings forth the question if people are actually willing to use them on a daily base and wider scale. When a password leaks, some damage could be done but the password can be changed and still be used in the future. Biometrics are non-changeable and cannot be revoked once they are compromised (Halevi et al., 2015). This can lead to insecurities in users whether they want to use such biometric systems.

According to research that has been done to determine factors that play a role in the user willingness to use biometrics (Halevi et al., 2015)(Habibu et al., 2021)(Byun & Byun, 2013)(Renaud et al., 2015), there can be multiple reasons that influence users on why and whether they want to use biometrics for authentication purposes. These factors all come forwards in the users' decision-making process. This decision making is almost always a trade off between the perceived benefits and 'cost'. The cost in these cases could be for instance privacy concerns, security concerns or experience.

One of the factors that is deemed to be very important is trust. When sharing your biometric data, users generally need to be convinced that the party they are sharing with is trustworthy. Public authorities, such as governments and educational institutions, are more trusted than for instance online shopping platforms (Halevi et al., 2015). Looking at the case of governments we can see that most countries already use a biometric passport, and thus forcing the users to share their biometric details with them (Habibu et al., 2019).

Another factor that may influence the trade-off between user gain and loss is the way the biometric authentication scheme is implemented. When using biometric technology like a fingerprint scanner is easier than for instance remembering and entering a traditional PIN-code, it may become more interesting for users to use that instead. In general, biometric authentication is also faster than the traditional ways (Byun & Byun, 2013). This will result in less effort for the user, and therefore increase the probability they want to use biometrics. Time saved is a great factor here, and also convenience is of importance.

One factor that is also really important to users according to different studies is the privacy concerns raised by using biometric authentication schemes. Privacy is very important for users in the sense that they want to be able to have control over the data they share with others. In the case of biometric data, the user is unable to alter this data once they are collected, since biometrics cannot be changed. Furthermore, biometric information contains a lot of sensitive, personal information. This may be a reason why users could be reluctant to use biometric authentication schemes. Large scale schemes will require big databases of users' biometric data, which will raise social issues (Byun & Byun, 2013).

Related to the privacy concerns raised is also the security of biometric systems. If the infrastructure and technological implementation is not secure enough, users will be less willing to use them. Previous experiences with security breaches also play a big role here. Users who have been hacked or had their data stolen in the past were less likely to share their biometric data (Halevi et al., 2015). The confirmation that the data being shared by the user is handled properly and in a secure manner is very important. This means that it is of great essence that the data is stored properly, e.g.,

encrypted. The hardware being used to extract biometric data also needs to be of certain standards, ensuring that they are tamper-proof and reliable. This all effects the users' willingness in actually using them.

Demographics are another example that will influence the decision making whether or not users want biometric authentication systems in everyday use (Habibu et al., 2021). Gender and age play a big part in the willingness of users. Younger people tend to be more willing to trust and use technical innovations such as biometric authentication schemes. Females are in general more willing to take risks than their male counterparts, and therefore have a bigger change that they will use these new systems.

2.5.1 How do users decide to use biometrics

Whether or not users decide to use biometrics is based on a lot of factors. The most important one of these factors remains the privacy issues incorporated with the use of biometrics. There have been several research and theories about how and when users are willing to give up certain aspects on their privacy level in order to gain some reward. The study of Li (2012) highlights two main trade-offs that influence the decision-making process of persons, namely the *privacy calculus* and the *risk calculus*.

This *privacy calculus* is a common approach to study a person's behaviour in certain decision-making processes. This theory suggests that consumers perform certain risk and benefit calculations, that will influence their decision. In this case the main risks are the privacy concerns that are raised by the use of biometrics, and the benefits are the advantages that using biometric authentication has to offer.

But most of the times people are not fully aware what is actually happing with their biometric data. This can be a huge influence in the trade-off whether or not to actually use the biometric authentication schemes in everyday use. The main privacy concerns that are raised are that biometric information is very sensitive and therefore it is very reasonable for people to be protective about them. Users could be scared off by the thought that this sensitive data is being used by the wrong parties or it falls into wrong hands in the case of a database breach or hack.

To further understand how users perceive certain risks and rewards regarding biometric authentication we can look at so called *mental models*. This is the term used to describe someone's thought process about how something works. When using biometric authentication, there are a lot of decisions to be made, and each individual will react different. This can have different causes, for example age, previous experience or expertise. When looking into the decision-making processes of persons about biometric authentication a few things can be concluded by previous studies. In the study of (Wolf et al., 2018) expertise about biometric authentication has been examined. While they thought that expert users were more reluctant to use biometrics, this was not the case. The motivations to use biometric authentication did differ from non-expert users though, mostly because of work related hardware and requirements.

2.5.2 Misconceptions

One very interesting aspect about using biometrics for authentication is the common misconceptions that still exist. This could also be a big factor for users when deciding whether or not they want to use such systems. Several studies (Wolf et al., 2019)(Lassak et al., 2021) have found that there are common misconceptions about using biometric for authentication purposes on mobile devices. One that really spoke out is that users are sometimes not fully aware what happens with their biometric data when using it on their devices. In the study by (Lassak et al., 2021) a system to replace

conventional passwords was investigated, called WebAuthn. This application offers the use of your smartphone as a way to offer two factor authentication, for instance with an unlocking mechanism like a PIN-code or pattern, but also allowing biometric schemes such as Apples TouchID and Android's equivalent. The user could be asked to provide for instance their fingerprint on their smartphone when logging in to a website, instead of entering their password.

One of the aspects that were studied was the user's knowledge about the storage of their biometric data. This was done by having multiple participants registrate using their biometrics, and later ask them to authenticate with them, using a made-up environment, and both followed by a survey. The study concludes that only 33% of participants correctly evaluated that their biometric data was only stored on their own device and therefore never shared with the environment that request the authentication.

This big misconception about the use of biometrics in authentication could be a substantial factor in users' mental model about using biometrics for authentication purposes. When considering the earlier mentioned *privacy calculus* where the trade-off has to be made between the privacy risks and the benefits, we might find that because of this and maybe other common misconceptions the privacy is not at much at stake as users might think. When looking back at the study of (Lassak et al., 2021), they find that 17% of the participants even believed that an employee at their made-up environment could access their data.

If such misconceptions were to be better understood by more potential users, the risk they believe they take may also decrease. Persons are probably more likely to use biometric authentication when they know the data is only stored on their own devices, than when they believe the data is controlled by the service they use.

2.6 Summary and relevance

In this thesis I want to take a closer look on how users perceive and use biometric authentication on their smartphones. In the previous sections we have seen that there are a lot of factors that come into play when using biometric authentication schemes. All these factors have their role in the user mindset and motivation to use biometrics on different occasions.

The need for authentication is ever growing and biometrics offer a fast and secure way to do so. We have seen that there are a lot of advantages in using biometrics, but there are some drawbacks. To ensure user privacy and security, we have shown that law enforcement has really increased over the years to facilitate the growth of biometric use. The way biometrics are incorporated in smartphones are also up to date and as secure as they can be.

This leaves us to speculate on the reasons why people would still be unwilling to use biometric authentication on their devices. This is probably based on misconceptions. This is the main motivation for the research question: *"What is the attitude of users towards biometric authentication for different types of online services?"* By researching this topic more and giving a better insight towards the thinking process of an individual regarding biometric authentication we hope to end some of these misconceptions.

3. Methodology

3.1 Data collection

The best way to gain an understanding of how people think about certain things it to ask them. This is why I have chosen to set up a questionnaire. The questionnaire was set up in such a way that we got insights in the quantitative numbers as well as more qualitative elements. Participants in the study were offered closed questions but were asked to provide a motivation for every answer given. The data was collected by means of a questionnaire on the platform LimeSurvey. This was chosen because it is hosted by the university itself and therefore does not rely on data being stored at any third party. The questionnaire was conducted in Dutch for it to be understandable for all age groups. It was spread by using different WhatsApp groups, family members, fellow students and by using social media to gain an as diverse audience as possible.

The questionnaire consisted of a mixture of closed and open questions. First there were some questions regarding demographics to have an insight in the sampling group. Then the participants were asked about ways they authenticate themselves in different situations and especially why they choose a certain approach. Questions were asked for different services, whether people would use their fingerprint on them and why they would or would not. Finally, we asked directly where people believed their fingerprint would be stored if they used it on their smartphones.

A copy of the questionnaire, translated to English, can be found in Appendix A.1.

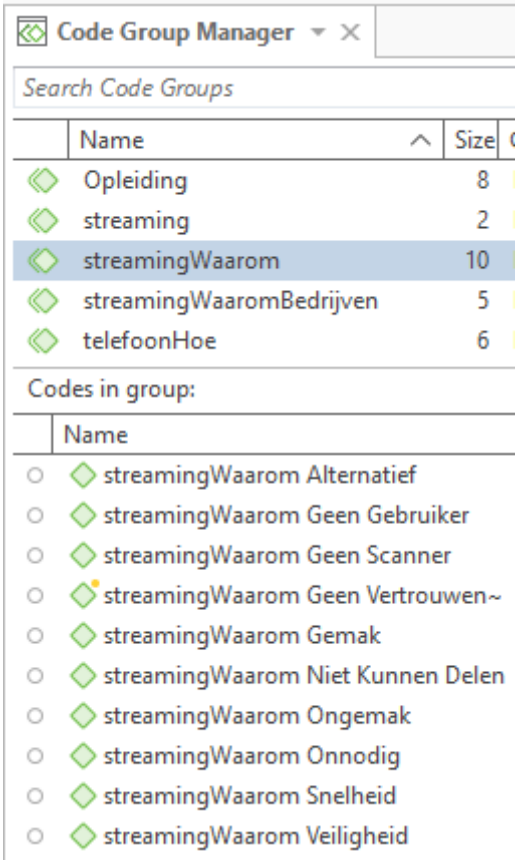
3.2 Data analysis

After having the questionnaire online for a few weeks, no more new responses came in and the number of responses we received seemed enough to have a solid basis for the rest of the processing. First, all full responses were exported to a Microsoft Excel file. This file was then altered a little bit to make it possible to import into the qualitive data analysis program being used, Atlas.TI. Atlas is a very powerful tool that enables coding the answers from each filled in questionnaire.

Every answer given to every response received their own code. This was done both automatically and manually. The multiple-choice question could be coded automatically, but all open questions had to be reviewed manually and then the decision was made which code was right to apply there. Because there were multiple questions that could have the same answer, such as ‘yes’ and ‘no’, or a motivation, the question was also incorporated into the code to keep track of how many times a certain answer was given per question. Some examples of codes being used were: *‘phoneHow Fingerprint’, ‘phoneHowWhy Speed’, ‘streaming Yes’, ‘streamingWhy Inconvenience’* and *‘streamingWhyCompanies To stop account sharing’*, to give you an idea about the build up of the codes.

After all responses were coded with the correct answer being given to a certain question, frequency analysis could be done. Atlas can count how much time a certain code is being used so we now know how many times a certain answer is being given. But even more important, we can use Atlas to count how many times combinations of answers have been given. For instance, the combination of all persons that are age of 41-50 and use their fingerprint to unlock their phone. This has proven to become very helpful in getting an idea for the reasons some persons thought about the biometric authentication concept.

The codes were then put in so-called code groups, with every question being their own code group. This resulted in a structure where we could filter questions and compare motivations with other code groups. To illustrate how this structure looks the following screenshot may be of help. It shows the code group of the question why people did or did not want to use their fingerprints to authenticate themselves if streaming services started to offer this option. The code group is called *streamingWaarom*, and below you can see the codes in this group, which were the motivations given by the participants.



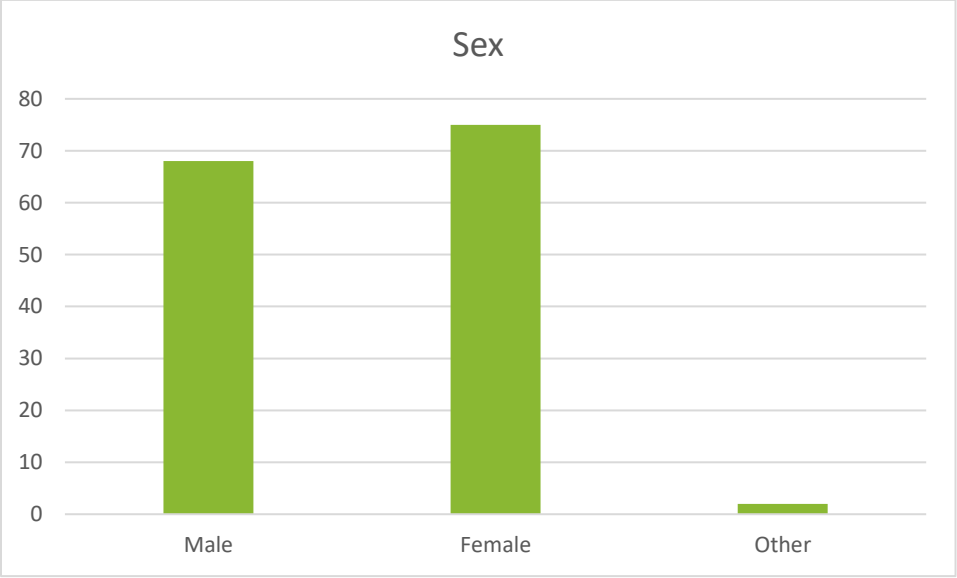
4. Results

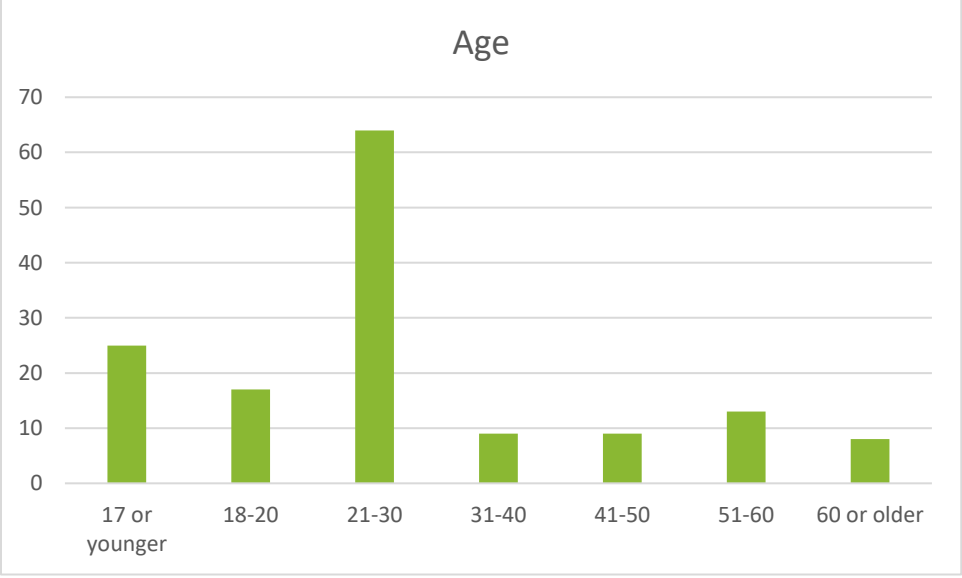
In this section the results of the online questionnaire will be shown and the findings will be explained.

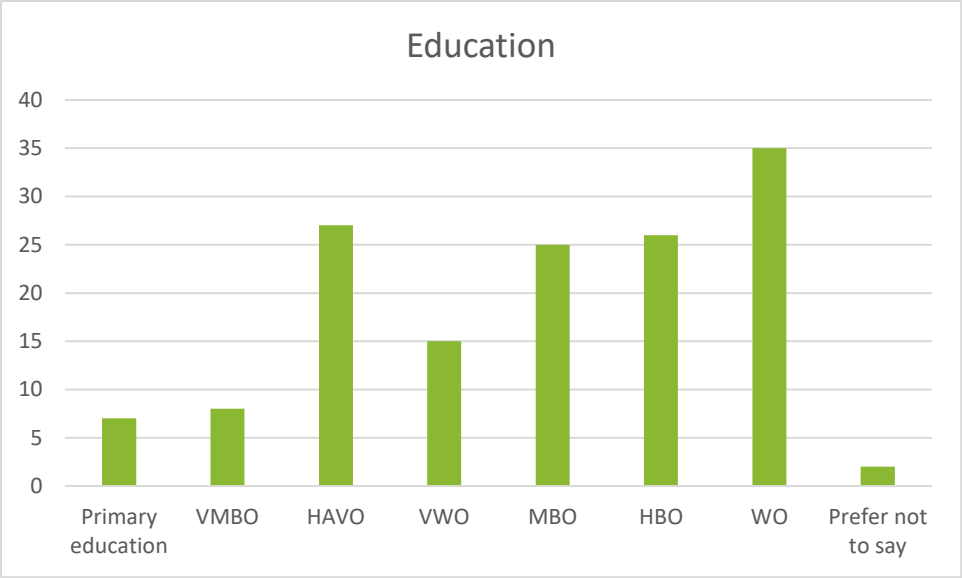
4.1 Population

The survey resulted in a total of 158 complete responses. After analysing the responses manually some responses were dismissed. The main reason for this was that people did not fill in any reasoning in the open questions, but instead just typed a dot or question mark. After these responses were filtered out, I was left with 145 fully answered surveys.

The aim was to spread the survey among as much diverse group as possible regarding age, sex and education level, to get an as broad as possible view of how people act with regards to their biometrics. This resulted in the following demographic graphs:



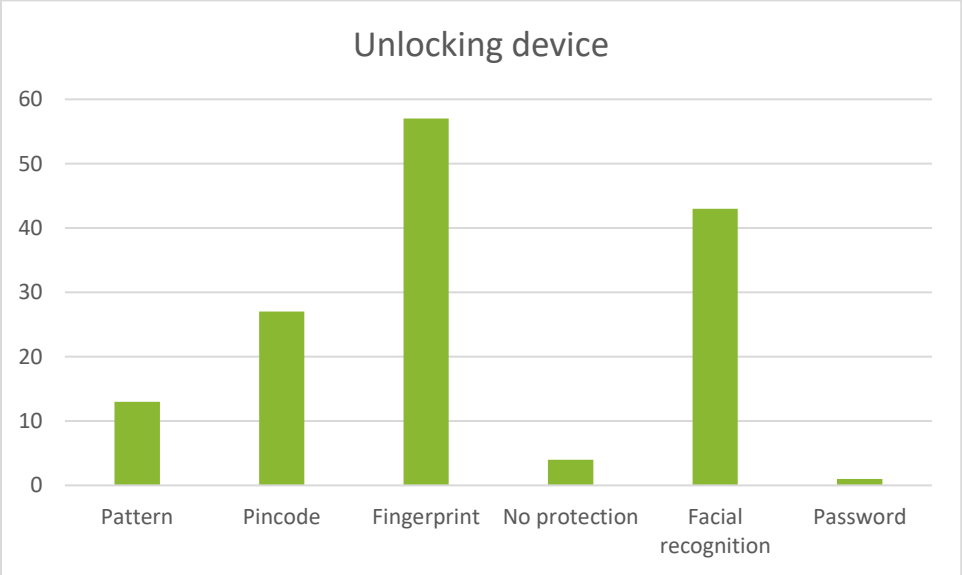


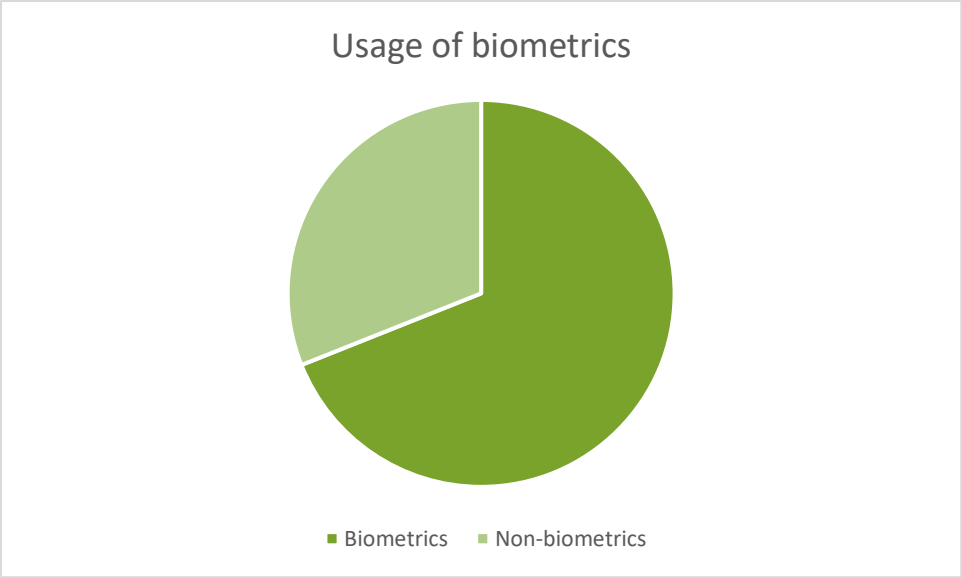


The spread among gender is close, with 68 participants indicating they were male, 75 indicating they are female and 2 indicating other. When looking at age we see that a majority of participants are between 21 and 30 years old, which can be explained by the way the survey was digitally distributed. The older age groups are probably their parents or other family members. The group of 17 and younger are probably the two middle school classes that filled in the questionnaire, who were asked to help by my mother who is a teacher there.

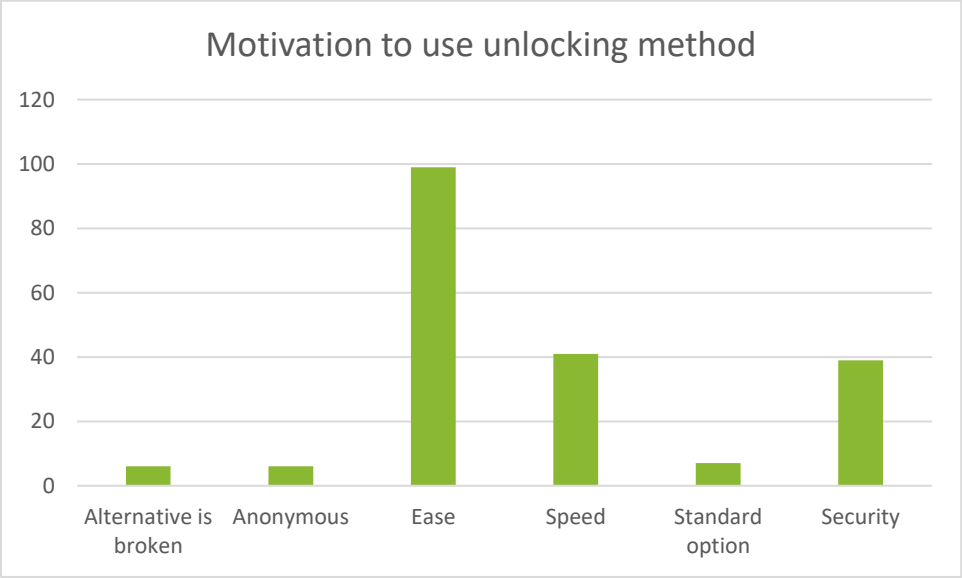
4.2 Usage of biometrics

The first thing that we want to establish is whether the participants already used some kind of biometrics on their smartphones and what the motivation behind their choices were. This was done by asking how participants unlock their smartphones. The majority of participants were using biometric options being offered.





When participants were asked about the reason they chose this way of unlocking their device, several reasons came to mind. Three main motivation points for people to choose their respective way of unlocking their phones were ease, speed and security. Because these questions were asked in an open-answer form, participants often indicated multiple factors. Therefore, the total count of motivations given does not add up to the size of the population of 145. This resulted in the following graph, which counts how much time a certain motivation was given.



Some notable answers being given in the motivation were:

"In case of emergency, a pattern is way harder to remember than a pin code", *"I don't have to share my pin code with the police when they ask, but they could use my fingerprints to unlock my phone"* or *"Everything else is broken on my device, so only a pin code remained"*.

4.3 Willingness to use biometrics on other applications

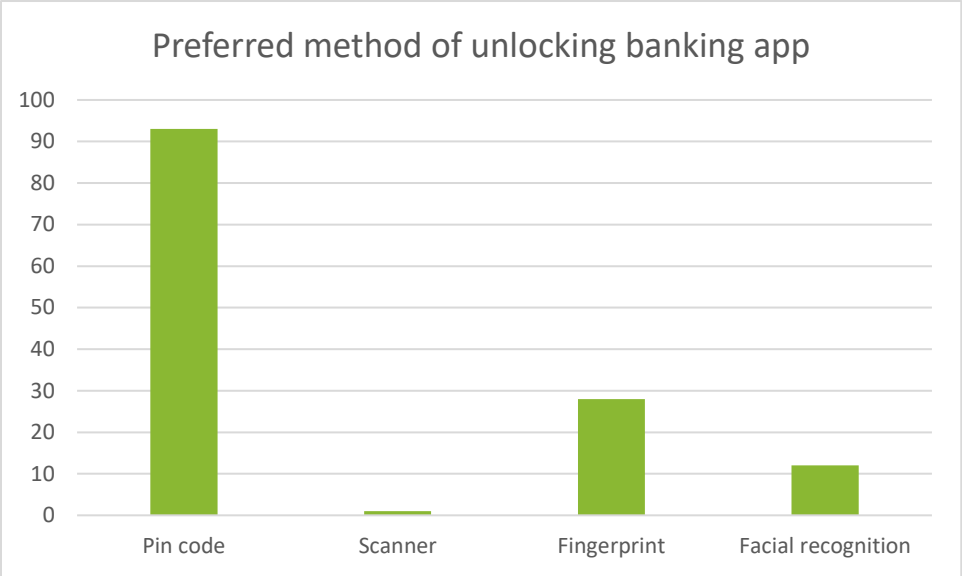
To further understand whether persons are willing to use biometric authentication options in other applications, several more questions were asked. The questions were about different types of applications, namely online banking, WhatsApp, the DigiD application and streaming service's application in general. Several online banking applications offer the possibility to use some sort of biometric authentication instead of the standard user-chosen pin code. WhatsApp offers users the option to unlock the application with their biometrics. On Android devices this relies on fingerprints, and on iOS devices this is can be done with facial recognition. The DigiD application uses a user-chosen pin code and does not offer an alternative. This question was therefore hypothetical, should the application ever consider implementing biometric options, like the banking applications do. The last questions were about streaming applications in general. There are many on the market and in the survey some examples were given like Netflix, Amazon Prime or Videoland. These applications do not require you to log in every time you open it, unlike the banking applications and the DigiD application, and also do not offer you the possibility to authenticate yourself using biometrics. Therefore, these questions were also hypothetical.

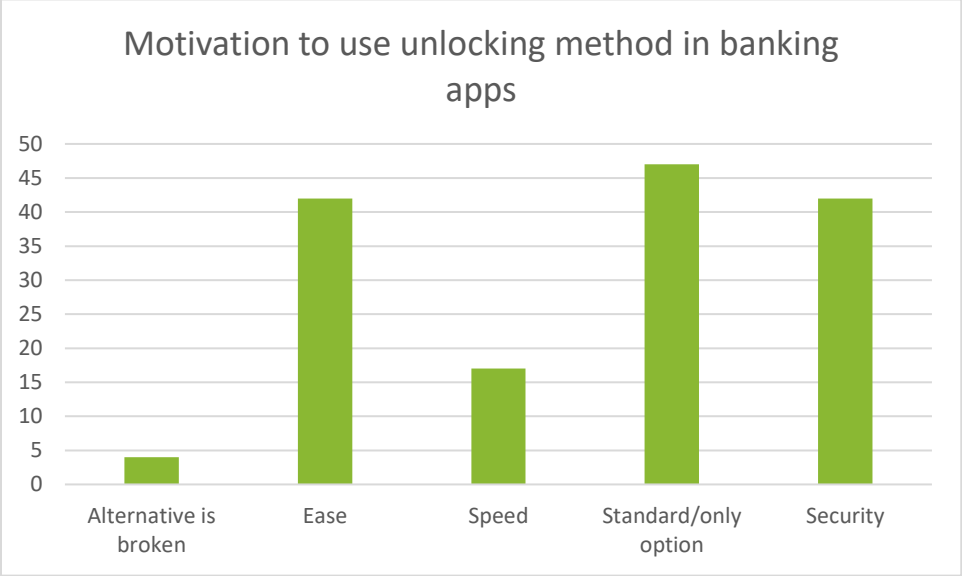
4.3.1 Banking application

First, we started asking if the participants used an online banking application. This resulted in 134 persons indicating they did, and 11 saying they did not. The people that do not use a banking application on their smartphone did not receive any further questions on this part. Of the 134 participants that did use a banking application the question was asked how they generally unlocked this application and why they chose this method.

The majority of people unlocked their banking application by use of a pin code, namely 93. Furthermore, 28 persons indicated that they used their fingerprint, 12 used facial recognition and 1 used a scanner or a similar device to unlock their application. When being asked about the motivation behind their decision, several reasons could be identified. One that stood out in this situation is the 'standard/only option' group. This motivation was given a total of 47 times. Out of these 47 participants, 45 used a pin code to unlock their banking application. This is an indication that not all banks support the possibility of using biometrics as an alternative in their applications.

The rest of the motivations being given were ease, speed, security or that their alternative is broken. A total of 42 participants motivated their choice by ease of use, 17 said it was due to the speed, 42 participants mentioned security reasons and 4 answered that the alternative option, like biometrics, is not working on their device. Some interesting answers were given here too, such as: *"I'm afraid my fingerprint will be abused when I am sleeping or drunk"*.

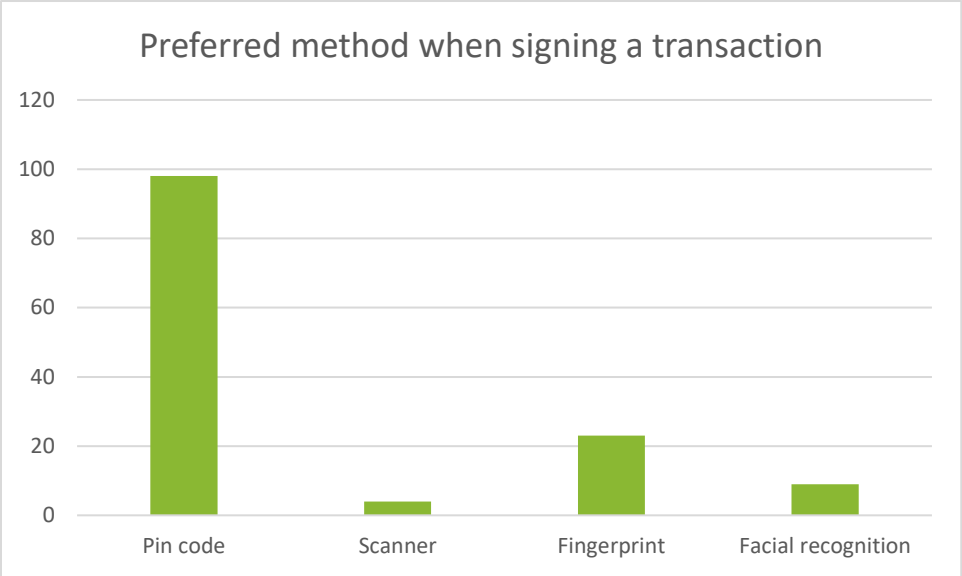


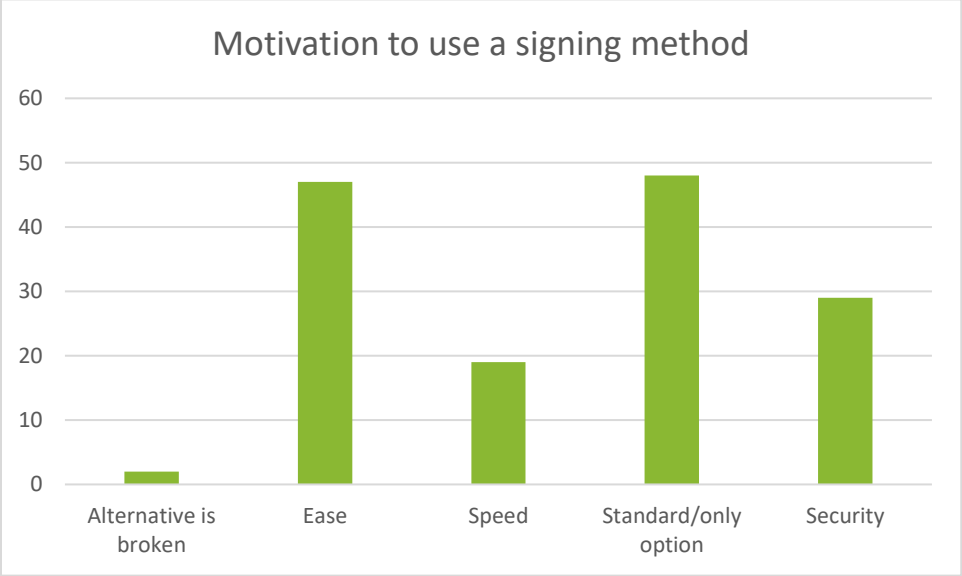


Next the participants were asked how they sign a transaction when using their banking application. Again, the majority indicated that they used a pin code, namely 98 persons. 4 persons indicated they used a scanner or other device to authorize transactions, 23 persons used their fingerprints and 9 mainly used facial recognition.

When asked about their motivations the same answers came up. 48 persons indicated that this was the standard option or the only option they had to sign a transaction. Ease was mentioned 47 times, speed 19 times, security 29 times and 2 persons indicated that the alternative they wanted to use was broken on their device.

Interesting was to see some persons indicating they used their fingerprints to log into the application, but when transferring money used a pin code and gave the motivation *"Force of habit".*



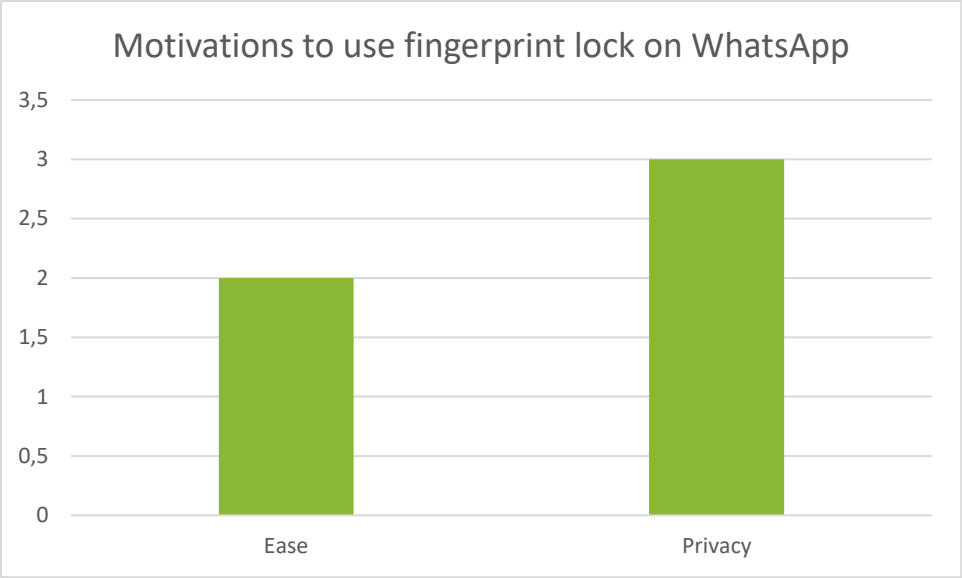


It is noteworthy to see that when doing a transaction, the biometric options were chosen less than when unlocking the application itself. Out of the 40 persons that indicated that they unlocked their online banking application using biometrics, so either fingerprint or facial recognition, 32 of them used this method to sign a transaction. This was mainly motivated by the fact that the application did not allow them to use the biometric option anymore or they felt more secure by using a pin code.

4.3.2 WhatsApp

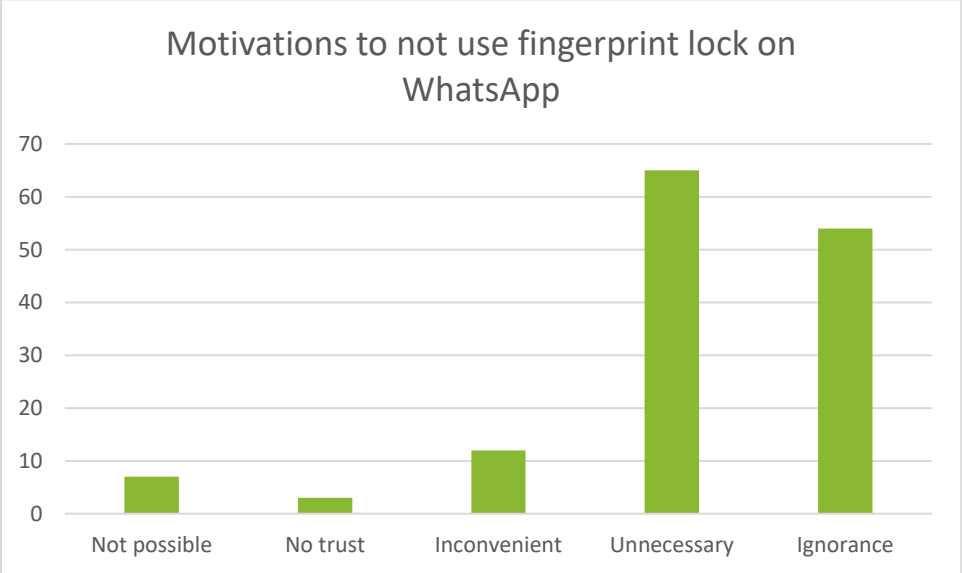
The next question was whether the participant used their fingerprint to lock WhatsApp. WhatsApp offers this option to users who want to protect their messages even more. Of the 145 persons, only 5 use this option. Again, the motivation about why they did or did not use the option was asked in an open question.

Of the 5 people that did use their fingerprints to lock WhatsApp, 2 indicated that this was because they found it easy to use, and 3 said it was because of privacy reasons.



The other 140 participants had several reasons for not using the fingerprint option on WhatsApp. 54 people indicated that they did know the option exist, 65 said it was unnecessary to have this function, 12 found it inconvenient or that it would be too much of a hassle to have, 7 indicated they could not use the function and 3 said that they do not trust WhatsApp with their fingerprints.

A lot of motivations given here were similar to *"Did not know this was an option"* or *"Not necessary"*.

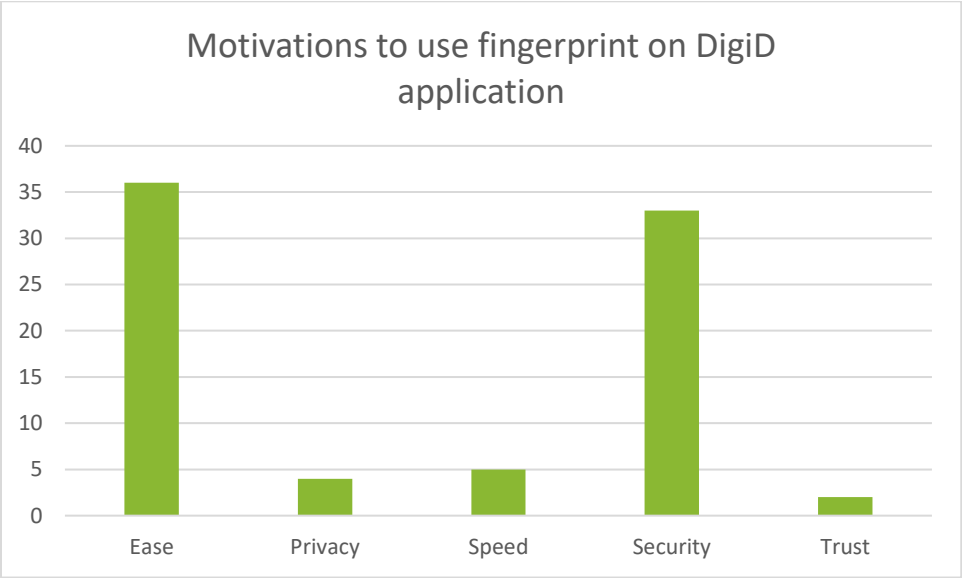


4.3.3 DigiD application

To use the Dutch government DigiD system to authenticate yourself on the internet somebody could use the DigiD application. This will enforce a two-factor authentication when logging in to DigiD enabled services. Users can also choose to receive a text message that contains a code for logging in. Depending on the service being logged into, two factor authentication is a requirement. For instance, when logging in to the *Belastingdienst*, you can still choose to just use your username and password.

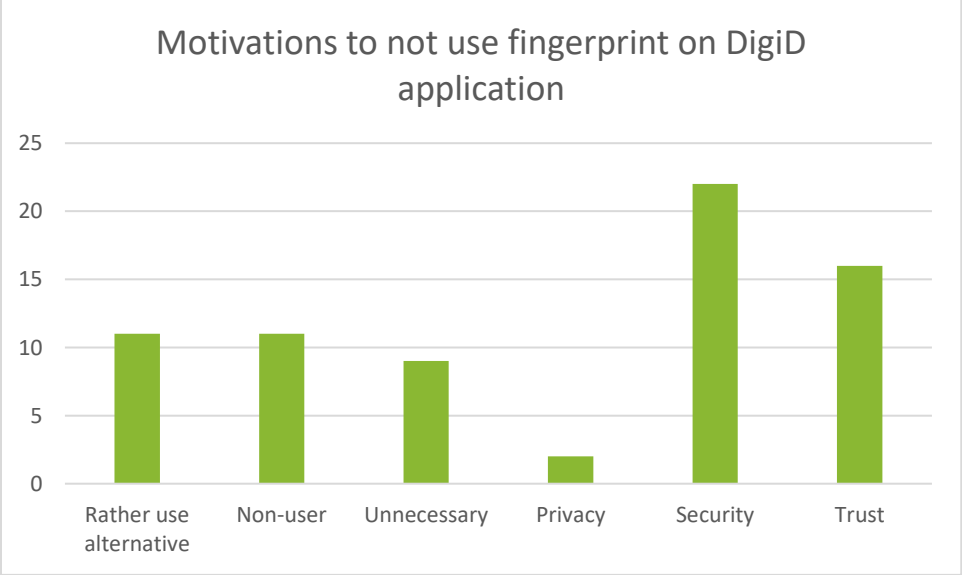
Users of the DigiD application have their own chosen pin code which they enter when using the application for two factor authentication. In the survey we asked the question if participants were willing to use their fingerprints instead, if this was possible. 76 participants indicated they would use this option, and 69 did not. The main reasons people would want to use their fingerprints on the

DigiD application were because it would be easier and more secure. Ease was referred to 36 times, and an increase of security was mentioned 33 times. 4 participants mentioned privacy as factor. Speed was given 5 times as motivation and trust were a motivation 2 times.



The motivations of the 69 participants that indicated that they would not use such option differed from the other group. The main concern was security issues, which was mentioned 22 times. Also, some sort of mistrusting was mentioned 16 times. 9 participants indicated that they felt it was unnecessary to have this option, 11 would rather have an alternative like a pin code, 11 participants indicated they did never use the application and 2 motivated their choices by privacy concerns.

Some interesting motivations given included: *"Imagine being unconscious and somebody getting access to all your government information"* and *"The only way the government gets my fingerprint is when I do something really bad"*.

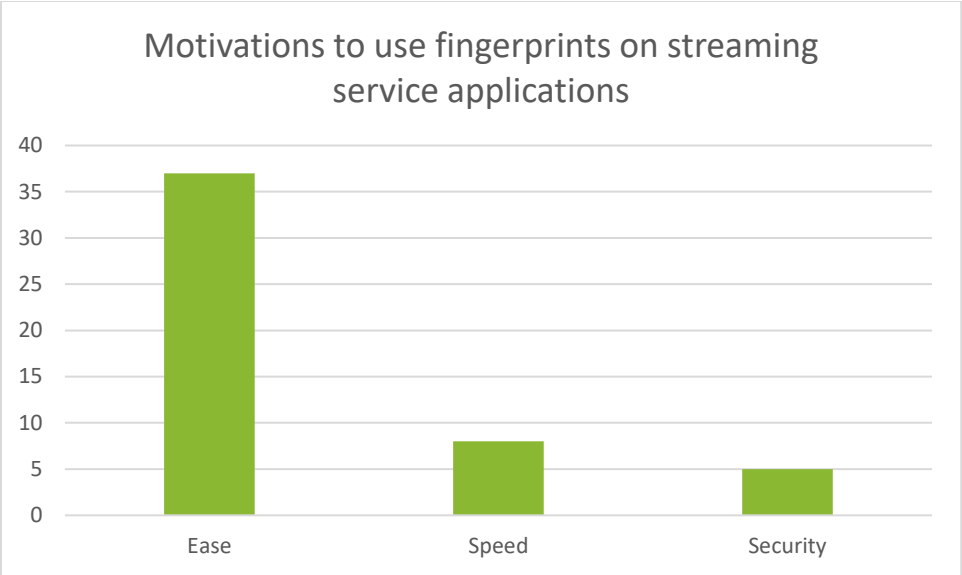


4.3.4 Streaming services

The next question was related to the online streaming services. No particular one was mentioned, but the examples of Netflix, Amazon Prime and Videoland were given. These applications all work

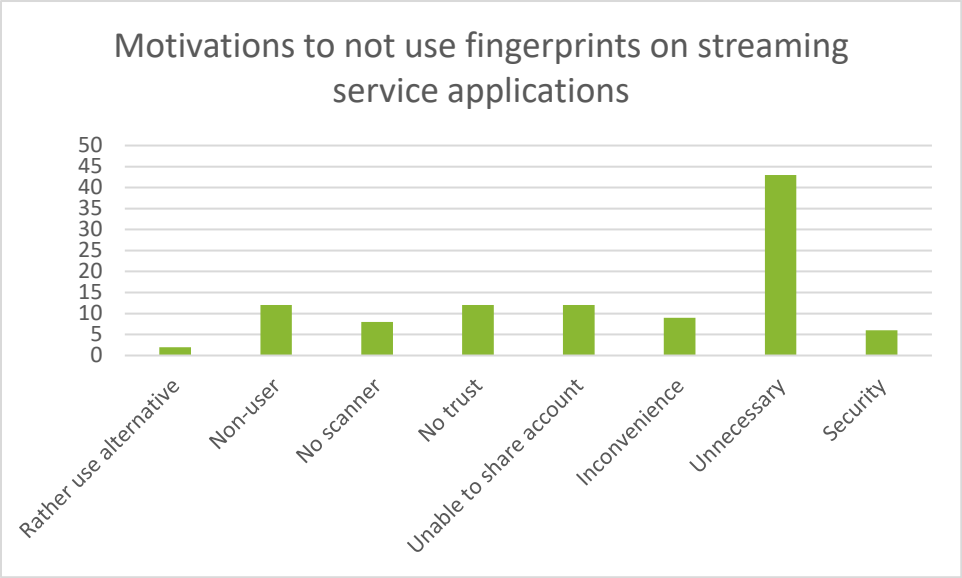
similarly, and do not ask users to log in every time to open it. There is also not an option to use any sort of biometrics available, so this question was also hypothetical.

Of the 145 participants, 47 would use their fingerprints to log in and 98 would not. The main reason to use their fingerprints given was ease, which was mentioned 37 times. Speed was mentioned 8 times and security reasons were given 5 times.



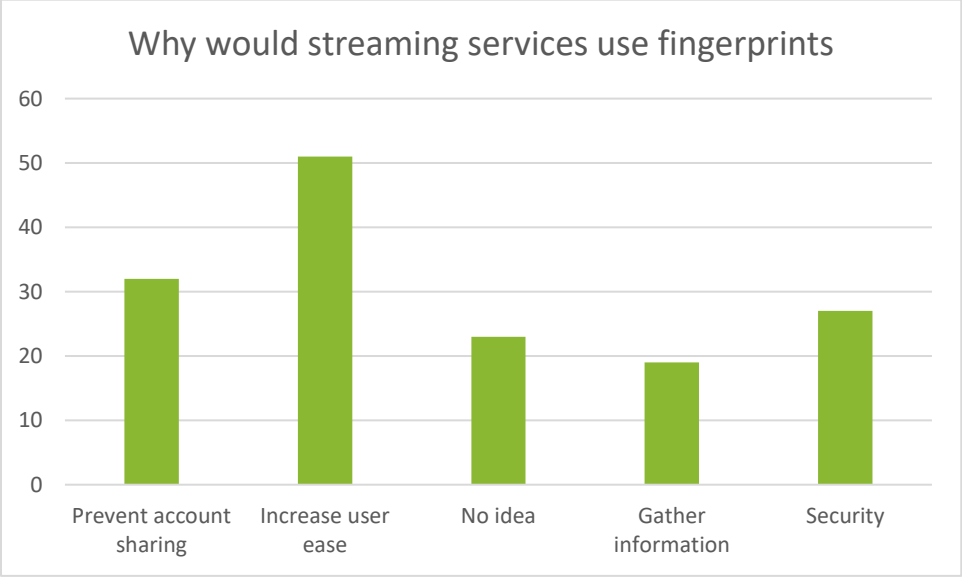
The 98 participants that would not use the fingerprint option if given had more different and diverse motivations. The main reason here was that participants felt it was unnecessary to have this option, which was mentioned 43 times. 2 participants would simply rather use an alternative and 12 indicated they were not a user. The motivation about not having a scanner was brought up 8 times by participants indicating that they used the streaming services on their TV, and therefore it had no scanner. Trust issues were mentioned 12 times, and 12 participants indicated that this would mean they would be unable to share their account. Inconvenience was also mentioned 9 times and security issues were mentioned 6 times.

As these motivations were more diverse, some interesting responses were given, such as: *"Banking and DigiD are well protected. These services are probably easier to hack"* and *"Those companies don't need to have my fingerprints"*.



Participants were also asked to find a motivation for the companies behind these streaming services to use fingerprints in their applications. The idea that the providers would do this to increase user experience or easiness and therefore keep the client happy was mentioned the most, at 51 times. A lot of people thought they would do it to prevent account sharing of some sort, as this was mentioned 32 times. Security motivations were mentioned 27 times and 19 participants thought the companies would use this to gather information. 23 participants indicated that they would have no idea what the motivation for companies would be.

It is interesting to see that a lot of people do not think in some kind of doom scenario but think the companies will do this to actually help the consumer. One participant for instance noted: *"A happy client is a paying client"*.

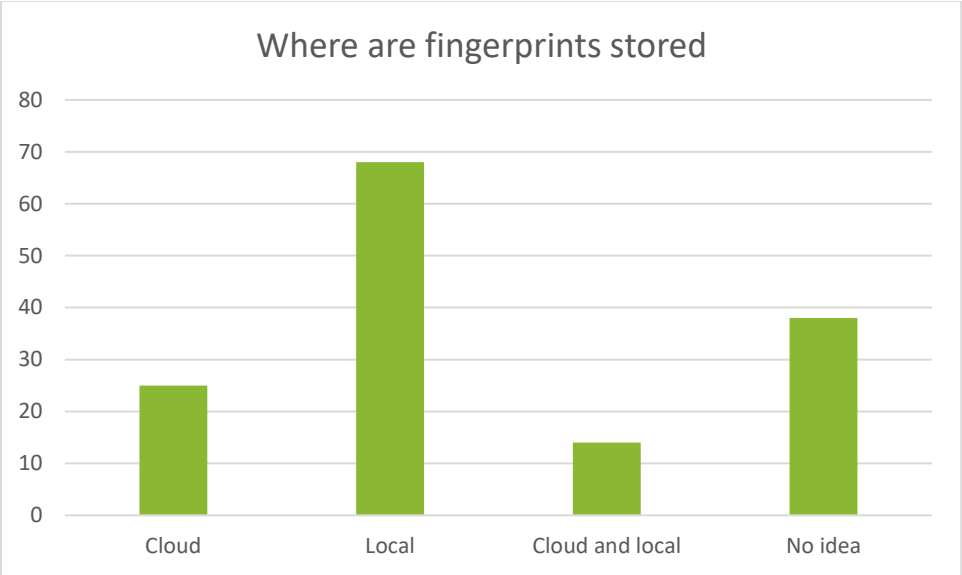


4.3.5 Fingerprint storage

The final question in the survey asked the participants where they thought their fingerprints would be stored if they used them. The results were quite surprising, as only 68 out of 145 persons correctly identified that the fingerprint was only stored on the local device. 25 people believed it was stored in some cloud location, the device manufacturer or at the service you use your fingerprint for. 14

participants believed it would be a combination between the two, so both locally and in a cloud or at another location. 38 persons indicated they had no idea what exactly happens to their fingerprints.

Some interesting responses were: *"I wouldn't be surprised if they store this on an offshore server-park somewhere in South-Georgia where law is so outdated, they can do whatever they want with them", "Places I do not want them to be"* and *"In my settings"*.



5. Interpretations and conclusions

5.1 Summary of results

When looking at the most important result that we got from the study we conducted, a few noticeable things jump out. When looking at the way people unlock their phone, we notice a majority in users that do use biometric options when available, namely approximately 69%. A lot of people do tend to act different when asked to use their biometrics in other applications if the possibility is being given. This could be due to the misconceptions of what happens with somebody's biometric data when using it on their smartphone (Lassak et al., 2021). When asked, only approximately 47% of participants correctly thought that their fingerprint was only stored locally on their devices, with the rest indicated they had no idea or that it was stored on another location, with possible access by a third party.

5.2 Interpretation and discussion of results

To further investigate the reasons why people tend to choose between their preferred way of authentication, we can combine different motivations and answers participants of this survey gave. One interesting thing to find out is if the group that mistakenly things their fingerprint is stored at a location other than their own devices is more reluctant to using fingerprints or biometrics in general. Of the 145 participants, only 68 knew that their fingerprint would never leave their own device, and a total of 39 believed it would be stored outside their own device. The rest had no idea.

Of the 68 persons that believed their fingerprints were only stored on their device, 49 used a biometric option to unlock their device. This is a percentage of approximately 72%. Of the 39 persons that were wrong about the storage location, 27 still used biometric options to unlock their device, giving a percentage of approximately 69%. This difference is not so noteworthy. Out of the 38 participants that indicated they had no idea what happened to their fingerprints, 24 used biometric options to unlock their device, which is approximately 63%.

From the rest of the results, we can see that a lot of people base their actions on misconceptions. Many people still believe that when having to use your fingerprint to unlock a streaming service, the service provider gets access to your fingerprint. This is of course never the case as this would be really hard to lawfully justify.

The usage of biometric options in different applications were a lot lower than the usage when unlocking the device in general. For instance, when asked if they would use it at the DigiD application was only about 52% and when with the streaming services only approximately 32% of participants would use this option. This difference may be explained by the misconceptions about the storage location and general trust in different organisations. This is in line with earlier studies like for instance that of Lassak et al. (2021) and Zirjawi et al. (2015).

From the study being done in this thesis we can therefore learn some lessons. When using biometric authentication on your smartphone, there is no need to be afraid of any privacy concerns. Your fingerprint will never leave your device and those who use it find it easier to use than the conventional passwords. The reason people still may be reluctant to use biometric authentication on their own devices is because of misconceptions.

6. Bibliography

Alsaadi, I. M. (2015). Physiological Biometric Authentication Systems, Advantages, Disadvantages and Future Development: A Review. In *International Journal of Scientific & Technology Research* (Vol. 1, Issue 1). https://www.researchgate.net/publication/322686764

Android Documentation. (2020). *Trusty TEE*. https://source.android.com/security/trusty

Arora, S., & Bhatia, M. P. S. (2021). Challenges and opportunities in biometric security: A survey. In *Information Security Journal*. Bellwether Publishing, Ltd. https://doi.org/10.1080/19393555.2021.1873464

Blanco-Gonzalo, R., Lunerti, C., Sanchez-Reillo, R., & Guest, R. M. (2018). Biometrics: Accessibility challenge or opportunity? *PLoS ONE*, *13*(3). https://doi.org/10.1371/journal.pone.0194111

Byun, S., & Byun, S. E. (2013). Exploring perceptions toward biometric technology in service encounters: A comparison of current users and potential adopters. *Behaviour and Information Technology*, *32*(3), 217–230. https://doi.org/10.1080/0144929X.2011.553741

Data Protection Act. (2018). European Parliament and Council, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)." In *Data Protection Act*.

Gruschka, N., Mavroeidis, V., Vishi, K., & Jensen, M. (2019). Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR. *Proceedings - 2018 IEEE International Conference on Big Data, Big Data 2018*, 5027–5033. https://doi.org/10.1109/BigData.2018.8622621

Habibu, T., Luhanga, E. T., & Sam, A. E. (2019). Evaluation of users' knowledge and concerns of biometric passport systems. *Data*, *4*(2). https://doi.org/10.3390/data4020058

Habibu, T., Luhanga, E. T., & Sam, A. E. (2021). A study of users' compliance and satisfied utilization of biometric application system. *Information Security Journal*, *30*(3), 125–138. https://doi.org/10.1080/19393555.2020.1813354

Halevi, T., Kuppusamy, T. K., Caiazzo, M., & Memon, N. (2015, June 16). Investigating users' readiness to trade-off biometric fingerprint data. *2015 IEEE International Conference on Identity, Security and Behavior Analysis, ISBA 2015*. https://doi.org/10.1109/ISBA.2015.7126366

Lassak, L., Golla, M., Hildebrandt, A., & Ur, B. (2021). *"It's Stored, Hopefully, on an Encrypted Server": Mitigating Users' Misconceptions About FIDO2 Biometric WebAuthn*. https://www.usenix.org/conference/usenixsecurity21/presentation/lassak

Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems*, *54*(1), 471–481. https://doi.org/10.1016/j.dss.2012.06.010

Matyás, V., & Ríha, Z. (2002). *Biometric authentication—security and usability* (pp. E1–E1). https://doi.org/10.1007/978-0-387-35612-9_23

Meng, W., Wong, D. S., Furnell, S., & Zhou, J. (2015). Surveying the development of biometric user authentication on mobile phones. *IEEE Communications Surveys and Tutorials*, *17*(3), 1268–1293. https://doi.org/10.1109/COMST.2014.2386915

Peng, P., Xu, C., Quinn, L., Hu, H., Viswanath, B., & Wang, G. (2019). What happens after you leak your password: Understanding credential sharing on phishing sites. *AsiaCCS 2019 - Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security*, 181–192. https://doi.org/10.1145/3321705.3329818

Renaud, K., Hoskins, A., & von Solms, R. (2015, November 20). Biometric identification: Are we ethically ready? *2015 Information Security for South Africa - Proceedings of the ISSA 2015 Conference*. https://doi.org/10.1109/ISSA.2015.7335051

Stokkenes, M., Ramachandra, R., & Busch, C. (2018). *Biometric Transaction Authentication using Smartphones; Biometric Transaction Authentication using Smartphones*. https://github.com/dasec/face-bf-btp

Wolf, F., Kuber, R., & Aviv, A. J. (2018). *How Do We Talk Ourselves Into These Things? Challenges with Adoption of Biometric Authentication for Expert and Non-Expert Users*.

Wolf, F., Kuber, R., & Aviv, A. J. (2019, May 2). "Pretty close to a must-have:" Balancing usability desire and security concern in biometric adoption. *Conference on Human Factors in Computing Systems - Proceedings*. https://doi.org/10.1145/3290605.3300381

Zirjawi, N., Kurtanović, Z., & Maalej, W. (2015). A survey about user requirements for biometric authentication on smartphones. *2nd International Workshop on Evolving Security and Privacy Requirements Engineering, ESPRE 2015 - Proceedings*, 1–6. https://doi.org/10.1109/ESPRE.2015.7330160

Appendix A

A.1 Questionnaire

This questionnaire is about the ways you secure your mobile device. I would appreciate it if you would fill in this questionnaire. Filling it in will cost approximately five minutes.

The answers and results will be analysed completely anonymous in my further research.

Thanks in advance for your time.

Kind regards,
Leon vd Boogaard

General questions:

These questions are there to know a little more about your background

***What is your gender?**

- Male
- Female
- Other

***What is your age?**

- 17 or younger
- 18-20
- 21-30
- 31-40
- 41-50
- 51-60
- 61 or older

***What is your highest achieved education?**

- Elementary school
- VMBO
- HAVO
- VWO
- MBO
- HBO
- WO
- Prefer not to say

Phone protection

To prevent unwanted access to your device you can lock your phone.

I am interested in how you have locked your phone, and especially the motivation behind this decision.

***How do you unlock your phone mainly?**

- A pin code
- A pattern
- A fingerprint
- Other, namely:

***Why did you choose this option:**

……

Banking applications

***Do you use an app for online banking purposes?**

- Yes
- No

***What way do use to log in to this app?**

- A pin code
- A fingerprint
- A scanner or similar device
- Other, namely:

***Why did you choose this option:**

……

***If you do an online transaction using this app, how do you sign it?**

- A pin code
- A fingerprint
- A scanner or similar device
- Other, namely:

***Why did you choose this option:**

……

WhatsApp

***WhatsApp offers the possibility to lock the app using your fingerprint to further protect your data. Do you use this?**

- Yes
- No

***Why yes/no?**

……

DigiD

***Suppose the DigiD app gives you the option to use your fingerprint as an alternative to a pin code or password. Would you use this?**

- Yes
- No

***Why yes/no?**

……

Streaming services

***Suppose online streaming services like Netflix, Amazon Prime or Videoland offer you the option to log in using a fingerprint. Would you use this?**

- Yes
- No

***Why yes/no?**

……

***Why do you think companies would offer this option?**

……

Fingerprint storage

***Where do you think your fingerprint is stored if you were to use it on your mobile device?**

Thank you

Thanks for filling in this questionnaire. All filled in response will be process fully anonymous and will be deleted when done. If you want to be kept informed of the results of my research, you can leave your email address (not obligated).

……

Any further remarks? (not obligated)

……