Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Architecture and Design
Department of Design

Carly Grace Allen

The Usability of Biometric Authentication in Mobile Phones

Master's thesis in Interaction Design
Supervisor: Associate Professor Sashidharan Komandur and
Professor Patrick Bours

June 2019

NTNU
Norwegian University of
Science and Technology

Carly Grace Allen

The Usability of Biometric Authentication in Mobile Phones

Master's thesis in Interaction Design
Supervisor: Associate Professor Sashidharan Komandur and
Professor Patrick Bours
June 2019

Norwegian University of Science and Technology
Faculty of Architecture and Design
Department of Design

NTNU
Norwegian University of
Science and Technology

Preface

This is a master's thesis in interaction design conducted at NTNU. This thesis was predominantly conducted in the spring semester of 2019 for a total of 30 ECTs and planned with preliminary research conducted in the fall semester of 2018 for 7.5 ECTs. The idea for this thesis sprung out of luck, with a friend asking me to participate in a study she was conducting and the resulting conversation for the study led to a discussion on what I might do for a thesis topic. As I have always found biometrics to be an interesting field but possessing little knowledge in the field, I decided to stop by the professor's office and talk about potential connections between interaction design and biometrics. After our discussion I went and talked to one of my professors and discuss further how I could make a thesis out of this conversation, and we decided on the relationship between usability and biometric authentication in mobile phones. These two professors then became my supervisors.

The completion of this thesis marks the fulfillment of the requirements for a Master's in Interaction Design from NTNU in Gjøvik. This report has been written predominantly for those who work in design, computer security, or biometrics. However, the hope is that others outside of these fields can use this as way to better understand the importance of both usability and security in mobile phones, to better understand what the research has said, and where it may go in the future.

This thesis is composed of seven sections. The first six sections relate to the introduction, background, methods, results, discussion, and conclusion of the research and work conducted for this thesis. Section seven consists of a related paper written based off of this thesis and submitted for publishing before the completion of this master's thesis.

NTNU in Gjøvik
01-06-2019
Carly Grace Allen

Acknowledgment

I would like to thank my supervisors Sashidharan Komandur and Patrick Bours for helping lead me down the right path and discovering an area that I am truly passionate about. Their help led me to learn so much about usability, security, and biometrics. I would also like to thank Frode Volden for being an outside opinion that I could talk to in the final semester of writing this thesis. I want to thank all of the participants during my survey and interviews for which this thesis could not have been completed without.

I also want to thank my family and friends for the support I've received throughout my schooling, and especially my mom. For if it had not been for her pushing me to study abroad, and for Ole Lund telling me about this master's program in the first place while I was studying abroad, I would not be here nor would I have found my passion. My life would be very different if I did not have the support from everyone around me, and I greatly appreciate it all.

C.G.A.

Abstract

There is often a perceived trade-off between security and usability. With an increase in the reliance on technology, it is becoming imperative to have both. Some of the reasons for the perceived trade-off between the two are that security and usability are often added on as "features" after the design and/or development of a system as well as a lack of consistent communication and understanding between those creating a system and those using it. One instance of the increasing importance of having both usability and security is in regards to mobile phones. Mobile phones have several different authentication methods available, including biometric authentication methods such as fingerprint, face, and iris recognition which are theoretically more secure and usable than other authentication methods. With mobile phones being used by people all around the globe with varying skills and technical comprehension, it is important to design and develop mobile phones that have authentication methods that are both secure and usable. Through this thesis, insights are gathered from a literature review, guidelines and principles researched, and a survey and interviews conducted to gain a better understanding and insights into current viewpoints, perceptions, and understandings of usability and security regarding mobile phone authentication. With this information, a set of 19 guidelines were created and tested as an evaluation method for biometric authentication in mobile phones as a way to increase both usability and security.

Sammendrag

Det er ofte en oppfattet trade-off mellom sikkerhet og brukervennlighet. Med en øke i avhengighet på teknologi, det kommer til å bli viktig og ha begge. Noe av grunnene for oppfattet trade-off mellom begge er at sikkerhet og brukervennlighet er ofte lagt på som "egenskaper" etter systemet har vært designet eller utviklet og at det er ikke nok kommunikasjon mellom de som skape et system og de som bruker systemet. En forekomst av for det er med mobiltelefoner. Mobiltelefoner har flere forskjellige godkjenning metoder tilgjengelig, og det inkludere biometrisk godkjenning metoder lik fingeravtrykk, ansikt, og iris gjenkjenning som er teoretisk mer sikker og brukbar enn andre godkjenning metoder. Mobiltelefoner er brukt av mennesker fra hele verden med forskjellige ferdigheter og teknisk forståelse, det er vitkig å designe og utvikle mobiltelefoner som har godkjenning metoder som er både sikker og brukbar. I denne masteroppgave, innsikt er samlet fra en literature review, forskning på prinsipper og retningslinjer, et spørreskjema, og intervjuer å oppnå en bedre forståelse av nåværende synspunkter, oppfatninger, og forståelser av brukervennlighet og sikkerhet angående mobiltelefon godkjenning. Med denne informasjon, 19 retningslinjer var skapt og tested som en evaluering metod for biometrisk godkjenning i mobiletelefoner som en vei å øke både brukervennlighet og sikkerhet.

Contents

List of Figures

List of Tables

Acronyms

UX	User experience
UI	User interface
HCI	Human computer interaction
HCISec	Human Computer Interaction and Security
HSBI	Human-Biometric Sensor Interaction
ID	Identification
TTP	Trusted Third Party
FAR	False acceptance rate
FRR	False rejection rate
EER	Equal error rate
UA	Universal access
FTE/FTER	Failure to enroll / Failure to enroll rate
FTA/FTAR	Failure to acquire / Failure to acquire rate
HB	Human Biometric
SUS	Security Usability Symmetry
NGOMSL	Natural goals, methods, selection language

Overview of Terminology

False acceptance rate (FAR)	Type I error or false positive; the likelihood that a system will accept another user as a genuine user
False rejection rate (FRR)	Type II error or false negative; the likelihood that a system will not accept the genuine user as the genuine user
Equal error rate (EER)	When the FAR and FRR are equal
Enrollment	The set up of biometric authentication where biometric information is collected and securely stored for later verification
Verification	Validating a specific user
Identification	Establishing the identity of one specific user out of many
Template	The biometric information that is captured during enrollment of biometric authentication
Noise	Something that is making it difficult to get a clear picture such as instability that is not part of the transmitted signal and is obscuring it
Distinctiveness	Being distinguishable or identifiable
Universality	Every person (or almost every person) that uses a system possesses it
Permanence	Something lasting or unchanging for a long period of time (or indefinitely)
Circumvention	Overcoming a problem or system
Universal access (UA)	Making technology that can be available to as many people as possible

1 Introduction

There has been debate as to whether increased usability decreases computer security and vice versa. Both are very important; if a system is not usable, then it will lead to a bad user experience (UX) and won't be used, and if a system is not secure, then it may not be used or can lead to security issues. This is especially true for mobile phones as they are used by people all over the world with different education levels, backgrounds, and experience. Mobile phones are a part of daily life for millions of people, and they are unlocked sometimes over 100 times a day (Griffin 2016). Mobile phones are used for alarms, storing contact information, figuring out where we are and were we want to go, gaining access to social media, accessing sensitive information such as banking or medical information, and so much more. With such an increase of reliance and accessing information that should only be seen by the genuine user, mobile phones should be more secure. This leads to the significant importance of mobile phone authentication being secure yet usable at the same time.

Biometric authentication in mobile phones has grown since the early 2000s, however it is not universally used as a security feature or authentication method. Many people rely on passwords, pins, and patterns; authentication methods that they are used to (Allen & Komandur 2019). But these methods are not the most secure options. Many people can't remember long pins and passwords, and there are only so many combinations that can be used for patterns and pins. A majority of people who use these authentication methods use pins that are only 4-6 digits long, short and easy to remember passwords, or simple patterns. And these methods can often be easily found out and understood just by watching a person unlock their phone or finding out important dates or names. Biometrics can be used as a more secure and easy to use authentication method, however today's biometrics are not flawless.

In theory, biometrics are both usable and secure; in practice, this is not always the case (Allen & Komandur 2019). That is part of the reason why biometrics have not been widely adopted even though they have been around for years in mobile phones. This study aims to develop a better understanding of how security and usability have been viewed and used in the past as well as how they can work together to make biometric authentication in mobile phones more secure and usable. An increased understanding in this can lead to making biometric authentication a better option for authentication in mobile phones and lead to an increase in security, usability, and satisfaction.

1.1 Keywords

Usability, biometrics, authentication, security, mobile phone, smartphone, user experience

1.2 Concepts explained

The main concepts discussed here are *usability*, *computer security*, *authentication*, and *biometrics*.

Usability can be defined by how “easy” an interface is to use against five components: learnability, efficiency, memorability, errors, and satisfaction (Nielsen 2012). The ISO definition further narrows the definition by focusing on three of those components: learnability (or effectiveness), efficiency, and satisfaction (Interaction Design Foundation n.d.). Usability is one important aspect of user experience, or UX, and a large part of the user interface, or UI. Here we will focus on the usability aspect, however the user experience will also be discussed to an extent.

Computer security can be defined as “the protection of computer systems and information from harm, theft, and unauthorized use” (Computer security 2019). This can be assessed via a risk analysis of a system. One way of implementing security in mobile phones is done with user authentication. Authentication is the process of verifying an identity as a genuine and intended user (Authentication n.d.). Authentication can be done via passwords, pins, patterns, and biometrics, among other things. When discussing computer security throughout this thesis, we will use computer security and security interchangeably and the focus of these terms will be on access control, which is one important aspect of security.

The word biometrics comes from two ancient Greek words, “bios” which means life and “metros” which means measure (Pocovnicu 2009). Biometric traits are used to uniquely identify a person based on physical or behavioral characteristics (the structure or the functions of the body). Biometrics allow a person to establish their identity not by what they possess or remember, but by who that person is (Böhm & Testor 2004, Pocovnicu 2009). Examples of biometrics can include fingerprints, face or iris recognition, voice recognition, gait, keystrokes, and signature.

1.3 Problem description

With mobile phones being used by so many people every day, there is an increased need for security and usability. If a mobile phone is usable but not secure, then sensitive or important information can easily be accessed by someone other than the genuine user. And if a device is secure but not usable, then even the genuine user may not be able to use the device and access their information. This is where many problems arise. Technology must solve both issues, and mobile phones have overall been lacking this connection between usability and security with regards to authentication. If biometric authentication specifically is to be used more often in mobile phones in the future, then this issue must be solved in a way that increases both usability and security at the same time.

In addition, there has been a lack of communication between usability and security experts as well as with the general population. Usability and security experts don’t always collaborate, usability and/or security are often added late in development or at the end as "features", and security experts don’t always communicate with the general population. What security experts and sometimes usability experts understand or perceive is often different from the general population, and this lack of communication is a large issue reducing use, understanding, and trust.

1.4 Justification, motivation, and benefits

Security has long been a concern when it comes to protecting sensitive or personal information. However, a large issue with security is that it is not inherently usable. There is a joke about computer security that a computer is secure when it's turned off, locked in a room underwater, and the key is thrown away. This helps illustrate the thinking around security that has been around for a while but is no longer as applicable as it was before. People need to have easy access to their information, yet everyone else should have a difficult time accessing the same information. The idea of usable security is about increasing both usability and security at the same time, and this can be a challenge. Some of the main reasons behind security problems are due to weak (or a lack thereof) credentials as well as physical attacks such as technology being stolen. If usability and security could both be increased, then these kinds of problems and concerns could be reduced. Building a stronger understanding of how usability and security have been perceived and integrated in mobile phones can help lead to the creation of more usable security.

One idea for solving security problems in mobile phones is biometric authentication. Biometrics don't need to be remembered or kept with a person at all times because they are based on who a person is, not what they have or remember. Nonetheless, biometric authentication is not perfect. In theory it is both usable and secure, but this is not quite true in practice. This is part of the reason why many people still rely heavily on simple passwords, pins, and patterns; people are used to them. In today's society, there is an ever growing importance for keeping easily accessible information secure, and biometric authentication could be one of the best options for mobile phones. Increasing usability and security in biometric authentication for mobile phones doesn't just benefit users, but it can also benefit those who develop these technologies.

1.5 Research questions

This thesis covers the scope of several research questions, which include:

- Can a relationship between usability and biometric authentication in mobile phones be expressed?
    - ○ Is there a trade-off between usability and security?
    - ○ How have usability and biometric authentication been evaluated in mobile phones?
- Are the perceptions from those working in the usability field and biometrics/computer security field in line with each other?
- Are the perceptions from those working in the usability field and biometrics/computer security field in line with that of the literature?
- Can usability and biometric authentication be more effectively incorporated in the beginning of the design and development process?

1.6 Contributions

Through this thesis, the researcher hopes to contribute insight into the research that has been conducted in usability and biometric authentication in mobile phones thus far, indications of the current understanding of usability and biometric authentication in mobile phones from several user groups, and use this information and more to create a set of guidelines for increased usability and security (or usable security) with regards to biometric authentication in mobile phones that can be used during the design and development of biometric authentication in mobile phones or used as an evaluation tool for prototypes or after implementation.

2 Background

2.1 Is there a trade-off between usability and security?

When computers were first invented, experts were the primary users. Usability was not considered because those experts were trained in how to use these systems, so the UX was not important. The security of these systems was the primary concern. Today, computers fit into our hands, come in various shapes and sizes, and have a wide variety of functions. Most people that use technology, especially mobile phones, are not experts, thus usability as well as security are important for users, even if they are not fully conscious of this (Allen & Komandur 2019).

There is a joke that is often used to describe a theoretically secure computer: "Computers are actually easy machines to secure: just turn them off, lock them in a metal-lined room, and throw away the key" (Cranor & Garfinkel 2005). This joke is often used to explain that there is a trade-off between security and usability. However, it is important to keep in mind that "the goal of security is not to build systems that are theoretically secure, but to build ones that are actually secure" (Tognazzini 2005). It is frequently thought that increased security leads to less usability, and increased usability leads to less security as they have different goals. Security can often be thought of as restriction, whereas usability can often be thought of as access (Yee 2005). One study states that even though usability and security should ideally support each other and that both should consider the user's workflow and behavior, there is indeed a trade-off between usability and security, and that it can pose major problems for system designers (Ben-Asher et al. 2009). Another study showed how the usability of software applications reduces security substantially (Alshamari 2016). One of the main reasons for this conflict is that security and/or usability are often considered or added only after a system has already been designed and/or developed (Sasse & Flechais 2005). Both usability and security should be considered early on in the development process, which can lead to the concept of usable security. Even though the trend of usability and security being at odds with each other is possibly starting to change, they still have different goals (Sahar 2013, Sasse & Flechais 2005). They are often treated as different realms "on account of their very different kind of nature" and having different meanings based on the current context in which they are being used.

Oluwatosin Nwokedi et al. (2016) wrote that "there has to be a trade-off between usability and security". The balance needed between the two is crucial when it comes to user safety; however, they found that user interfaces for authentication often encourages either secure or insecure behavior depending on its requirements. One part of their discussion was explaining the criteria that can be used for evaluating the usability of a system (convenience, understandable, inclusivity, and requirement) and criteria to evaluate the security of a system (revelation, secrecy, privacy, breakability, and abundance). "A prevalent understanding is that usability criteria must be sacrificed to achieve meaningful security criteria, and vice versa" (Oluwatosin Nwokedi et al. 2016). Nevertheless, it is important to go past just adopting principles of usability and to discuss both usability and security together in the beginning, not independently. The outcome of a system that is able to balance both security and user interface design (or usability) will have great benefits, even though not much has been done to address this (Oluwatosin Nwokedi et al. 2016).

Garfinkel (2005) argues that "there are many instances in which security and usability can be synergistically improved by revising the way that specific functionality is implemented". There are many times when there is no inherent trade-off between the two; it just takes more work. Traditionally, usability and security have been seen as antagonistic towards each other, but a reason for this could be due to the fast evolution of technology, leaving little time to focus on usability as well as a lack of communication between security and usability in the past. Cranor & Garfinkel (2004) wrote that the " 'received wisdom' on the inherent conflict between usability and security goes against common sense". They continued with that common sense dictates that usability and security ought to go together and that systems that are not usable won't be used, while systems that aren't secure will become useless. But building a secure system does not ensure its security; a system also needs to be installed and operated correctly and securely (Bishop 2005). And for this to be accomplished, the principle of psychological acceptability can be used. This is not an easy feat, and it "depends upon the context in which those mechanisms are to be used" (Bishop 2005).

Humans are prone to making errors, so interface design should be made insensitive to those errors as much as possible (Cranor & Garfinkel 2005). That is one of the principles of usability: to reduce the number of potential errors that a user can make (Nielsen 2012). Security and usability can work in harmony with each other when systems interpret user desires correctly (Yee 2005). An area of study that has arisen from the usability and security debates is called HCISec: the study of human-computer interaction and security together. There are multiple approaches to usable security among HCISec researchers: 1) building systems that "just work" without users having to intervene (reducing user errors), 2) "develop[ing] security and privacy-related metaphors that let users intuitively use security or privacy software correctly" (learnability and efficiency), and 3) giving and teaching users knowledge that is needed to use security and privacy tools effectively (learnability and memorability) (Cranor & Garfinkel 2005). Cranor & Garfinkel (2005) believe that a final solution for reducing user errors will most likely be a combination thereof.

Yee (2004) discusses how taking a different approach to security in the design of a system or product itself can help avoid conflicts between usability and security. Yee (2004) makes several points, including the main points of security and usability being incorporated into the design process, that security and usability can be viewed as having the same goal (fulfilling user expectations), and that "an essential technique for aligning security and usability is incorporating security decisions into the users' workflow". One view is that conflicts arise between usability and security when a system doesn't have the necessary information to ascertain if a particular result is wanted. This means more potential errors, thus reducing the usability of a system.

Discussions about a trade-off between usability and security often don't go into detail. Many believe that there is a trade-off, but don't say "how much security you're going to get, here is a precise statement of how much [something] helps in terms of security, and here's how much it hurts in terms of usability" (Sasse et al. 2016). Many use the concept of a trade-off as an excuse to not precisely say what the security benefits are and in what scenarios that usability is burdening (Sasse et al. 2016). However, the idea that "in many cases, you're actually improving security by increasing usability" is becoming more prevalent. One belief is that "if a feature isn't working for users, it will ultimately undermine security". Users make bad decisions and errors when their ability to make decisions are taken away, which reduces their satisfaction (one of the principles of usability).

There is a divide between what users and what security experts see as best practices for staying secure online, which is part of the problem; there is almost no communication here. Usability, user experience, HCISec, and usable security are all fairly new fields, so there are many misconceptions, misunderstandings, and miscommunication around these fields. "We don't see enough researchers stepping back to ask what a person actually needs to do [to be more secure] and how we can make that the most usable thing" (Sasse et al. 2016). However, even though these fields are still fairly new, there has still been some research conducted in these areas.

Some researchers have written guidelines for creating more secure designs. Yee (2002) was one of the first to create a list of design principles for both interaction design and security. These principles include: path of least resistance (should also be the most secure way), appropriate boundaries (interface should show distinctions between objects and actions), explicit authority, visibility, revocability (or undoing), expected ability (should not make users think they can do something that cannot be done), trusted path, identifiability, expressiveness, and clarity. Another study discussed establishing foundations for developing mental models to bridge the gap between security and usability (Mohamed et al. 2017). However, Mohamed et al. (2017) said that there is no universal formula for reducing the "apparent paradox between usability and security". The idea of making a system that is easy to use while also making it hard for intruders to get in to is the main problem when it comes to the intersection of usability and security; the human factor.

It is a common belief that the weakest link in information security is the users, or humans themselves (Sasse & Flechais 2005, Patrick et al. 2005). It is often said that "security is only as good as its weakest link, and people are the weakest link in the chain" (Sasse et al. 2001). To create more usable security, we need to go beyond security and UI into human factors and behavior, or the human part of security (Sasse & Flechais 2005). Sasse & Flechais (2005) discuss two things that should be kept in mind when designing secure systems that people can use: "designers can assume that users will not comply with policies and mechanisms requiring behavior that is at odds with values they hold", and that "the role of security is a supporting one", not a primary role or goal. Usability models can be applied to most products or services, however, there is no singular security model that can be applied to most products or services.

One study discussed finding the "right" trade-off between usability and security with a design model that was created based on a usability inspection model followed by a case study on how to use it (Braz et al. 2007). The study states that security is often thought to only be related to system functionality, that it is independent of usability, and that usability or the UI is like a layer that just sits “on top of the ‘real’ system’ ”. This is one cause for many of the problems between usability and security. Braz et al. (2018) stated that “to be able to build reliable, effective and usable security systems, we need specific guidelines that take into account the specific constraints of usability mechanisms and their potential consequences on security”, to which they wrote about the Security Usability Symmetry (SUS) model that deals with that very issue.

Schultz et al. (2001) developed a taxonomy to organize the issues of usability and security methods to make a “strong case for the need of systematic usability analyses for the development of usability metrics for information security”. In the end, the study states that human intervention in the judgment of what actions to take and in the performance of implementing those actions is needed. The human factor has often not been taken in to account. Another study proposed a security and usability threat model that details the important factors for the usability and security of secure systems as well as a process for assessing those systems (Kainda et al. 2010). The security-usability threat model includes evaluating: effectiveness, satisfaction, accuracy, efficiency, attention, vigilance, motivation, memorability, knowledge/skill, social context, and conditioning. HCISec developed from HCI due to the need to improve the usability of secure systems, but Kainda et al. (2010) states that many systems are still “being designed without enough consideration of usability”. Usability and security have a close relationship with each other, and improving one may improve the other.

Mihajlov et al. (2011) presented a “quantification approach for assessing usable security in authentication mechanisms... to guide the evaluation process of authentication mechanisms”. The study discussed how usability evaluation methods do not factor in security issues, thus are not sufficient for evaluating security. Mihajlov et al. (2011) evaluated an authentication method with a security evaluation based on secrecy, abundance, revelation, privacy, and breakability, and with a usability evaluation based on processing depth, meaningful retrieval, requirements, convenience, and inclusivity. Cranor & Buchler (2014) believe that “to achieve usability gains without sacrificing security, researchers must go beyond adopting human-centered design principles and embrace user decision making”. Their study talks about three types of command relationships between users and systems to increase both security and usability. Cranor & Buchler (2014) believe that developments in usable security may need command relationships between the user and the system to evolve and that researchers need to accept user decision making to be able to reach gains in usability.

A study conducted by P. Kukula et al. (2010) discussed the human-biometric-sensor interaction (HSBI) evaluation method. The purpose of this model is to combine metrics from biometrics, ergonomics, and usability for the purpose of evaluating the overall performance of a biometric system. P. Kukula et al. (2010) evaluated the HSBI evaluation methodology with regards to fingerprint authentication. The study showed that the HSBI method can provide feedback and analysis to help system designers and implementers better understand if issues are a result of a system, users, both, or something else. This helps increase the understanding of the usability and security of a system. Braz et al. (2018) developed ten usability factors as a part of their seven-step process in increasing usable security for the design process of user authentication services. These factors included: efficiency, effectiveness, productivity, satisfaction, learnability, safety, trustfulness, accessibility, universality, and usefulness. They then broke these principles down to: minimal action, minimal memory load, operability, privacy, security, load time, and resource safety. Braz et al. (2018) used the original ten factors, task scenarios, and their corresponding usability criteria (the broken down factors) and security problem or threat as an evaluation tool.

Throughout all of this, one concern that arises seems to be around the word "trade-off" itself. When hearing the word trade-off, many people go straight to a negative connotation. The definition of trade-off is "a balancing of factors all of which are not attainable at the same time" or "a giving up of one thing in return for another", both of which are more negative (Trade-off n.d.). Another important concern is the understanding of usability and security. Yee (2005) writes, "security and usability are qualities that apply to a whole system, not features that can be tacked on to a finished product" which is a common misconception that often leads to the belief of a trade-off. Yee (2005) said "attention to usability concerns is always necessary to achieve true security".

Based on this research, there is an overall common belief that usability and security are linked to each other, and this link is not necessarily negative like the connotation of the word trade-off often produces. Security is not being communicated to users which is part of the issue here; users aren't security experts, so they just don't understand (Sasse et al. 2016). Security and usability should be designed and built into systems in the beginning during design and development, not just added after development is complete and before (or sometimes even after) release (Cranor & Garfinkel 2005, Alshamari 2016, Sahar 2013, Yee 2004, Oluwatosin Nwokedi et al. 2016, Sollie 2005). Incorporating both usability and security in the beginning would allow them to work together more harmoniously and can reduce potential trade-off between the two. Cranor & Garfinkel (2005) wrote a book called *Security and Usability*, and the whole premise of the book is that security and usability can work in harmony with each other. Overall, there are still those who believe that there is a trade-off between usability and security, however, the trend is moving more towards the idea that when they are incorporated properly and early on in the design and development stages that they can work together, influence each other, and even support each other. More usability can increase security when done right without there necessarily being a trade-off.

2.2 Biometric security

Security doesn't need to be complex. And security doesn't always mean that we should look at things in terms of "we need a lock on that door"; sometimes, security means "we don't even need a door there" (Sons et al. 2017). And whether there are several doors or a lack of doors, access needs to be regulated. One important point of security is to restrict unauthorized access. The threat of unauthorized access to devices is most often combated by user authentication (Rogowski et al. 2013). One study states that the usability of an authentication method is related to the time to learn, the speed of performance, subjective satisfaction, and the rate of error by users and the system (Sollie 2005). However, many people do not put as much stock into securing their phones as they do with other things such as computers or even cars because a mobile device is something that many carry with them at all times and use constantly. This can bring a false sense of security, which could be a reason as to why there are still many people who do little to secure their mobile phones, if anything at all. Adams & Sasse (2005) discuss how a "majority of users [are] security conscious, as long as their perceive the need for these behaviors".

Before delving into biometric security specifically, it is important to also discuss privacy. Privacy relates strongly to security, and having authentication and security measures can help ensure privacy. It is a value that many people have that is individually subjective and socially situated, but it is frequently not a primary task for users (Ackerman & Mainwaring 2005). When it comes to privacy and security, "there is likely to be a gap between what we know we must do socially and what we know how to do technically", or a social-technical gap (Ackerman & Mainwaring 2005). There are often five privacy pitfalls: obscuring potential or actual information flow, emphasizing configuration over action, lacking grained control, and inhibiting established practice (Lederer et al. 2005). When security information is conveyed clearly and carefully, these pitfalls can be avoided, leading to increased security and privacy. And to help avoid these pitfalls, informed consent is important. For users to feel a level of privacy and security, they should be able to "opt-in" to these policies (Friedman et al. 2005). Friedman et al. (2005) states that informed consent should involve disclosure, comprehension, voluntariness, competence, agreement, and minimal distraction. Informed consent and privacy are very important when it comes to authentication as an aspect of security, and more so with biometrics than with other forms of authentication due to the type of information handled.

The user authentication process should require the least amount of user interaction necessary, procedures should be unobtrusive, should involve almost no user input, and should be intuitive (Braz et al. 2018). Traditional authentication methods are more obtrusive, often require more input, and are not as intuitive as biometric authentication methods. For biometrics to be used as an authentication method, there are two modes: the enrollment mode (when biometric data is obtained and stored), and the authentication mode (biometric data is obtained again and verified) (Böhm & Testor 2004). There are also two types of authentication: verification (one-to-one matching) and identification (many-to-one matching) (Coventry 2005). When it comes to mobile phones, verification is the primary type used. Biometric authentication is not like passwords, pins, or patterns where it is either correct or not. Biometrics require statistical analysis and are accepted based on a curve (Coventry 2005). The effectiveness of the analysis can depend greatly on the quality of the template collected during enrollment.

There are two types of errors that are important when it comes to biometric authentication: the false rejection rate (FRR) (rejecting the actual user) and the false acceptance rate (FAR) (accepting an imposter). These are two of the main aspects that are important when designing biometric authentication systems. If an authentication system is very secure, it will most likely have a higher false rejection rate, making it more difficult for genuine users to get access. This in turn can make it more difficult for imposters to get access. Yet, if an authentication system is less secure with a lower false rejection rate, then genuine users may have an easier time accessing the system, which leads to more usability. There is also a higher chance of a false acceptance, which would allow imposters to get access more easily to the system, which leads to potential security risks.

There are many benefits to using biometrics instead of standard user authentication methods such as passwords, pins, or patterns. Biometrics actually authenticate the user themselves, they cannot be passed on to someone else or stolen like keys, cards, passwords, or other types of authentication, they cannot be lost (except under rare conditions) or forgotten, and they can have a very fast authentication process (Matyas & Riha 2002). Biometrics can be used to determine with relative certainty that the user is there when the biometric data is collected (Pocovnicu 2009). They can effectively identify one person out of a large population, and they are also unforgettable and cannot be lost since it is about the individual, not memory. A user can't share their biometric data like they can with a password, and biometrics can be more cost-efficient in the long run. When users are required to have many passwords and to change them often, it can often lead to users writing down and disclosing passwords, which shows reduced usability and leads to a decrease in security and security motivation (Adams & Sasse 2005). These problems are not as relevant to biometrics, but when it comes to security motivation, it is important to look at user motivation to help educate users and prevent privacy and security issues with regards to authentication (Sasse et al. 2001).

Biometrics also have disadvantages. Noise, distinctiveness, and non-universality are three issues when it comes to biometric systems (Böhm & Testor 2004). Noise refers to noisy biometric data such as if a person has a cold leading to issues for voice recognition or a cut or wet finger for fingerprint recognition. These issues can lead to false rejections which can be very inconvenient and frustrating for users, which in turn reduces efficiency. Distinctiveness refers to the fact that biometric traits are usually assumed to vary between individuals, but there could be cases where two people have similar biometric data (such as twins or siblings for facial recognition) which could lead to false acceptance of an imposter or someone other than the genuine user. And non-universality is about not being able to attain certain biometrics from every user. Accuracy, false acceptance and rejection, the potential of failure to enroll, and the data not being considered private are a few other disadvantages and concerns (Matyas & Riha 2002).

On top of that, each biometric trait has its own pros and cons. Each one can be evaluated based on universality, uniqueness, permanence, collectability, performance, acceptability, and circumvention (Pocovnicu 2009). Universality is about each person being able to use that biometric, uniqueness is about how unique the biometric is from one individual to the next, permanence is about how well it can withstand the aging process, collectability is about how easy it is to acquire the biometric without inconveniencing the user, performance is about accuracy and robustness, acceptability is about the approval by users, and circumvention is about the ease of falsifying the biometric trait. To help combat these disadvantages, biometric systems could have liveness testing, tamper resistance, secure communication, security threshold levels, and a fallback authentication method (Matyas & Riha 2002).

Mobile phones (predominantly smartphones) can have biometric systems integrated in two ways: “as a biometric collecting device or as a stand-alone system to protect unauthorized use” (Pocovnicu 2009). This means that mobile phones are collecting biometric data and sending it via internet to be processed and matched to the stored data, or the entire biometric system is located in the mobile phone and is used to protect functions and data in the mobile phone itself from unauthorized users. This can make mobile phones much more secure than standard pins, passwords, patterns, or other standard security options, which is becoming more important each year due to users using their mobile phones to access and store secure banking information, work information, personal information, and more.

There are often four aspects in the evaluation of biometric systems: performance, acceptability and user satisfaction, data quality, and security (El-Abed et al. 2010). These evaluations of biometric systems often do not take into account the user’s perceptions or the human aspect of them, just the satisfaction and acceptance of the system. There is a lack of evaluation methodologies taking in to account users and their perceptions which is a large drawback for biometrics. Gathering this kind of information can lead to a better understanding of user needs and improve biometric systems’ quality which could increase user understanding as well as user adoption. When studying user perceptions of biometrics, El-Abed et al. (2010) state that it is important to keep in mind: socio-demographic factors, learnability and memorability, trust, ease of use, privacy issues, physical invasiveness, and cultural issues. Overall, respondents of a survey considered biometric technology to be a more appropriate than knowledge-based solutions (such as passwords, pins, and patterns) against fraud and that a trust factor is very important (El-Abed et al. 2010). “Even if the performance of a biometric system outperformed another one, this will not necessarily mean that it will be more operational or acceptable”. The main drawback in the spread of biometric technology is the “lack of a generic evaluation methodology that evaluates biometric systems taking into account: performance, users’ acceptance and satisfaction, data quality and security aspects”.

The perception of biometric security is also important when it comes to the usability of it. If the general perception of a system is negative due to a lack of usability, trust, or satisfaction, it will not be used. Acceptability (and in turn trust) is an important usability concern that must be addressed for a system to be widely used (Sasse 2004, Patrick 2004). There are several trust models that have been developed, and Patrick et al. (2005) developed a list of "Trust Design Guidelines" in order to make it "easier for designers to identify those elements capable of promoting trust and those capable of destroying it" when it comes to designing systems. Helping users understand biometric systems would most likely increase user acceptance and trust of biometrics, and this understanding could likely come during the enrollment process in the interface (Patrick 2004).

Most research on perceptions of biometrics has been conducted in the western world (Riley et al. 2008). The study conducted by Riley et al. (2008) discussed a cross-cultural examination of user views of biometrics, attempted to understand how people's perceptions of biometrics can change from culture to culture, and attempted to understand how concerns regarding biometrics can affect its implementation. Countries that show high individualism, low uncertainty avoidance (meaning that they are more tolerant of the unknown), and low power distance (meaning the acceptance of unequal power distribution within a population) were predicted to be more likely to accept biometric technology than those with low individualism and more collectivism, less tolerance for the unknown, and more acceptance of unequal power. The survey was conducted in India, South Africa, and the United Kingdom to attempt to see if there are strong cultural differences in acceptance of biometrics and if it correlates to their prediction based on Hofstede's five cultural constructs. Respondents from India overall had the most positive responses to biometrics about ease/speed of use, security, and acceptability which did not fit with the prediction previously stated. The United Kingdom had less positive responses to biometrics, with respondents believing that token authentication and passwords were more acceptable than biometrics. South African respondents had similar views to those from India, however, it was to a lesser extent but still positive. Across all three countries, the willingness to try biometrics was high, yet security and fears regarding health and safety were concerns that arose from the study. These two concerns were strong predictors of willingness to use biometric systems, and ease of use, knowledge of biometrics, and perceived security were predictors, although to a lesser extent than security and health concerns.

Al Abdulwahid et al. (2015) created a survey to better understand user's perceptions of security and usability. In the study, they found that 82% of respondents preferred to have some form of authentication which can lead to the perception that those users, and potentially a majority of users overall, understand that having some form of security is important with internet connected devices. The study also found that about 94% of respondents experienced issues with authentication at some point and that it can be quite annoying for users when authentication fails (reduced efficiency). This is especially important to consider when users are authenticating multiple times a day, where a majority of respondents stated that they used authentication methods ten or more times a day. Respondents were also asked about what authentication methods were most usable, and the Android pattern unlock was rated most usable, then the iOS Touch ID (fingerprint biometric) was rated as the second most usable option. The following question was about confidence in storing their biometric data with a trusted third party (TTP), and 41% of respondents felt confident or very confident with storing biometric data whereas 30% did not feel confident with doing so. This study shows that trust has not been fully established when it comes to biometric authentication.

Zirjawi et al. (2015) created a study to better understand what users think of biometrics, trust in biometric authentication, perceived usability and privacy trade-offs, and to see if demographic factors had any influence on those results. When asked about trust in different security authentication methods, a large majority trusted passwords and pins (78%) followed by iris and fingerprint recognition (59% and 58% respectively). A large percentage of respondents stated that they did not trust face or ear recognition for authentication. Storage of biometric data is often discussed, and many respondents believed that the collection and storage of fingerprint and facial recognition data were critical or very critical (69% and 66% respectively).

Another study conducted two surveys: one to understand customer perspectives about adopting biometric authentication systems for online payments and financial services, and the other to understand the perspectives from the financial industry on biometric authentication in the same field (Lovisotto et al. 2017). The results between the two surveys were quite different, with 85% of customer respondents having a positive view of biometrics (focused on fingerprint and facial recognition) and only 36% of industry respondents having a positive view or experience with biometrics. This could shed some light on one possible reason why the adoption of biometric authentication is still not common practice. Following the survey, Lovisotto et al. (2017) developed a five-factor framework including modality performance, usability, interoperability, security, and privacy for deploying biometric systems in mobile environments in relation to financial services. However, even though the framework was developed with financial services in mind, it may be able to be applied to other use cases as well.

In general, it can be concluded that there is an overall belief outside of the security profession that security is important (Al Abdulwahid et al. 2015, Zirjawi et al. 2015, Lovisotto et al. 2017). Al Abdulwahid et al. (2015) found that the importance of security is followed closely by privacy, and then by convenience. Zirjawi et al. (2015) found that along with security, data protection and privacy in smartphones is just as important. However, there is reduced trust in unpopular or uncommon biometric authentication types such as ear recognition. Even though users seem to find security important, they do not tend to take all of the steps suggested to secure themselves and their devices. When it comes to security, it is especially important to remember that the idea of "one size fits all" security does not take into account different scenarios and use cases, so it is important to have options and to support the user rather than restrict them (Tognazzini 2005). Al Abdulwahid et al. (2015) believe "that whenever the benefits of adopting any proposed solution are clearly elaborated and justified, it would gain higher level of acceptability" and use. And this leads to the usability of biometric security.

2.3 Usability and biometric authentication in mobile phones

Usability issues can stem from hardware, software, interface design, and/or users. Usability issues with regards to biometric authentication are partially due to the detection error trade-off curve. Passwords, pins, patterns, and tokens are either right or wrong; they are not based on a curve, just 100% correct or not. However, with biometric authentication, captures for each authentication attempt are never 100% the same, thus are determined based on a curve. Each authentication attempt is compared to the template that was collected during enrollment, and depending on the threshold that has been established, a score will be provided and an attempt will either be accepted or rejected based on that score. The threshold can be established based on the equal error rate (EER), and it comprised of the false acceptance rate (FAR) and the false rejection rate (FRR) when they are equal to each other. The FAR and FRR are inversely related, meaning that when one is high, the other will most likely be low. Having a low equal error rate usually equates to a more accurate authentication system. The problem that often occurs here is that if the system has a high threshold and high equal error rate, then a system can be perceived as less usable because the genuine user will most likely have a more difficult time being authenticated.

Brostoff (2017) believes that the reason biometrics are not the default authentication method today even though biometrics in laptops and phones have been around since the early 2000's is because of user experience and usability. It is easy to use methods that we are comfortable with (such as pins and passwords), but unless there is a shift of focus to user experience and usability, biometric solutions won't become a part of daily life yet. It has been estimated that almost all smartphones in 2018 have some form of biometric authentication available (Find Biometrics 2016), but how many of those mobile phone users regularly use biometrics for authentication? "For the consumer, using biometric authentication isn't noticeably different to what they're already doing" (Brostoff 2017). New technology should actively improve something, not just be new or 'cool', which can be a reason for the slow adoption of biometric authentication. Usability can improve biometrics, and the combination of the two can make authentication more 'invisible', compatible, and faster than traditional authentication.

There are multiple factors that can help increase the usability of biometric systems. Sensors are smaller, more reliable, and more ergonomic, biometric algorithms are better, feedback can be provided during use, and they are being integrated to provide a more seamless use and environment (Patrick 2004). However, accuracy and its relation to convenience is still a usability issue when it comes to the physical usability. To get accurate readings, some authentication systems take more time than others, which heavily reduces convenience and can thus reduce user satisfaction.

Ashbourn (2000) created a list of user characteristics that can be used to predict the performance of biometric systems. These characteristics include: acceptance of biometric concepts, knowledge of technology and computers in general, familiarity with biometric characteristics, experience with the specific device being used, the environment of use, and transaction criticality. Coventry (2005) states that “developers must work with an iterative design and evaluation process to create successful biometrics applications”. To improve the usability of the enrollment process, which is sometimes a user’s very first introduction to biometric authentication, the enrollment process should include education to the user about the biometric trait itself, training to enable consistent use of the biometric technology, an explanation of the interface support, the use of a trainer, and supervised “playtime” (Coventry 2005).

Biometrics can be more usable than authentication based on memorization or tokens, thus are a good choice for authentication in universal access (UA) systems (Mayron et al. 2013). There is much potential for integrating usability and security together effectively with regards to biometric authentication in UA systems that traditional authentication methods have not been able to do. A common usability issue is that systems are created in ways that are not intuitive to users, and security is no exception to that. Security is important, and by making users more aware of security tasks to perform, why they are important, how to perform them, and how they can prevent errors or problems, the usability of a system can increase and can in turn increase the security as well (Mayron et al. 2013). Mayron et al. (2013) described a list of usable security principles that are built from a combination of security and usability principles and research. Those principles consist of least surprise, good security now, standardized security policies, consistent and meaningful vocabulary, consistent placement of controls, and no external burden (Garfinkel 2005). Including these principles in the design process can help increase the usability and security of a system at the same time.

Even though acceptance of biometric authentication is increasing, the benefits are not always visible to users, which can cause users to be wary or not use biometrics (Patrick 2008). If biometric authentication systems do not inform users about what they are doing, how the information is collected and stored, and do not explain how it is secure and private, then the usability can be reduced. One of the five principles of usability is learnability, and if biometric systems don’t explain what is going on, then they are not learnable and can easily lead to errors or non-use (Nielsen 2012). Lack of information and understanding has been seen as a large issue in the adoption and acceptance of biometric authentication and to the learnability of biometric authentication methods. If something is not socially acceptable, appropriate for a given environment, filling a perceived need, fundamentally understandable, usable, and not destructive to personal privacy, then that can hinder perceived usability, security, and actual use of a system (Coventry 2005).

If users don’t understand the reason for using biometrics or security in general and do not trust them, then the usability may not matter. Some users may also not want to use their biometrics due to concerns about safety, privacy, or even religious reasons (Sasse 2004). If what users expect of biometric systems doesn’t match with what the system actually does, then there is even less incentive to use biometrics as an authentication method. If users don’t trust biometric authentication or don’t think that their privacy is protected, then it won’t be used, even if it has a high level of usability.

A common usability concern regarding biometric authentication is when users are temporarily or permanently unable to use or enroll in a specific biometric authentication option (Sasse 2004). Failure to enroll (FTE/R) and failure to acquire (FTA/R) are two important metrics to consider for usability (Coventry 2005). If users fail to enroll in a system, then it cannot be used and will lead to a poor user experience, thus is not usable. Outliers must have a fallback strategy, and there must be some form of exception handling to offer a way to bypass the issue of failure to enroll or failure to acquire data that is still secure and acceptable. If the fallback strategy is just to use a pin or pattern after a number of failed attempts, then the system cannot be considered very secure. 5% of the population is estimated to have unreadable fingerprints, blind users cannot use iris biometrics, and if a user has a burn or cut on their finger or face, then users may not be able to temporarily use those biometric (Sasse 2004). Providing alternatives can be critical for accessibility and usability.

A very common problem with usability, and usability in biometric authentication systems as well, is that those who create a system or design often think that it is intuitive and that users will easily understand; that is rarely the case (Allen & Komandur 2019). There are few things in the world that are inherently usable. Biometrics is not one of them, which is why biometric authentication systems need to have usability and security incorporated throughout the entire design and development process, several of which ways have been discussed. If this is done, then it will lead to an increased understanding and acceptance of biometrics, and to do this effectively, there must always be usability testing.

2.4 Usability testing and evaluations

Usability testing is conducted to understand the usability of a product or system, often (but not always) from the potential users point of view. To do this, representative users are found (a variety of those who might use the product or system) and they are observed to understand how they are using a system, where they succeed, and where they may be struggling (Nielsen 2012). One of the most difficult and important things to do during usability testing is to not ask leading questions or input personal thoughts or opinions, because that will skew any data collected, introduce bias, and will not be representative of what users think. There have been a handful of studies to better understand the usability of biometric authentication, where only a few of them have focused on mobile phone environments.

Before delving into usability testing and evaluations of biometrics, it is important to remember that authentication systems (and systems in general) should be evaluated on several criteria. Renaud (2005) discusses quality criteria and environmental considerations for authentication. These criteria include accessibility, memorability, security, and cost. If a system works well but has a high cost, it may not be implemented. If the security is too low, it may not be implemented. If a system has low memorability (such as passwords or protocols that are very complex and/or must change often), then it may not be implemented or used well. If a system is not accessible, then it is preventing its own use.

There are three categories that usability tests and evaluations can be placed under: 1) test - making use of representative users to work on typical tasks using a system where performance is measured, 2) inspection - usability experts inspecting usability-related aspects of a UI, and 3) inquiry - collecting information regarding user' preferences, desires, and behaviors to formulate the requirements for a design (Braz et al. 2018). Most research discussed here focuses on the test category. One study conducted a usability evaluation on handwriting biometric authentication (Blanco-Gonzalo et al. 2013). The usability evaluation consisted of testing three different angles of use for an iPad, three different styluses, and no training was provided to the users. The authors believed that it was important to understand how a user's signature might change throughout the different sessions and time that the method had been used. This is important because with any new tool, it takes users time to adjust and get used to the way that the tool or system works. Following the ISO usability definition, data was collected that showed over time, the effectiveness and efficiency (two usability aspects) increased due to a decrease in errors from the first session to the third, regardless of which angle and stylus was used.

Another study conducted a usability test on two specific mobile phones with biometric authentication as well as a survey to investigate experiences using biometric authentication in mobile phones in everyday life (Bhagavatula et al. 2015). In the evaluation, the users already had positive perceptions of biometrics and some had previously used biometric authentication on their mobile phone. Pin, Android face unlock, and iPhone fingerprint were all tested in multiple scenarios including sitting, sitting in the dark, walking, walking with a bag in the other hand, and after having used moisturizer. The users rated each scenario and authentication method to be easy, and the iPhone fingerprint was the preferred authentication method at the end of testing. In the survey, few people stated that they were not comfortable with their biometric data being stored. This study found that convenience and usability were important factors in the adoption of biometric authentication. Usability itself seemed to be a driving factor of whether or not users decided to use biometric authentication or not.

There was a study that conducted a usability test for voice, face, and gesture recognition with a total of six conditions conducted in a random order with thirty users (Trewin et al. 2012). Three practice trials and eight memory task trials were completed by each participant with a device that was designed to accept all attempts as being successful so that the usability of the method itself could be tested. The combination of face and voice (where users had to say a code out-loud and take a photo) had the highest (FTER) at 10.3% as well as the highest failure to acquire rate (FTAR) at 21.3%. Overall, the two conditions that required multi-factor authentication methods provided the most difficulty for users, where one user abandoned one of the multi-factor conditions after 2 frustrating attempts and three other users were unable to provide face or voice samples to pass the initial enrollment phase. Overall, the study found usability issues with every method and condition. A different study conducted a survey to understand the user experience, expectations, and satisfaction of smartphone authentication (Ahmed 2017). The study found that fingerprint was the most preferred authentication method (40%), followed by pattern (22%) and password (17%). Fingerprint and pattern authentication also had the highest satisfaction levels due to their ease of remembrance (memorability) and use, though fingerprint authentication was overall considered more secure than pattern authentication by the respondents.

The HSBI method is a method that utilizes components of usability, ergonomics, and sample quality for the evaluation of functionality and performance of biometric systems (P. Kukula et al. 2010). Another study created improvements to the H-B (human-biometric) interaction methodology as well as a handful of usability evaluations (Gonzalo 2016). Gonzalo also discussed accessibility in biometrics with elderly and people with disabilities and found that time was a key factor in the usability of biometrics. Mobile phones can boost biometrics and usability because many of the ways that we authenticate with biometrics are things we already do, such as taking a selfie, pressing a button, or using a stylus. There have also been other usability evaluation studies for mobile devices or tablets focusing on face recognition, multimodal biometric systems, iris recognition, and for signature authentication among others. Another way to evaluate biometric systems is through a list of guidelines for the design, implementation, and evaluation of authentication methods on smartphones for future developments such as that developed by Attaullah et al. (2017). The study created a list of 17 guidelines, ranging from explaining the purpose and methodology of a study and its data collection, classifier training guidelines, inclusion of failure to acquire and failure to enroll rates (FTAR & FTER), considerations about testing time length, and including initial usability evaluations (for example the System Usability Scale).

All of these are methods that are most often used after a product or system has already been designed and/or developed. Braz et al. (2018) created a seven-step process in their book called "Integrating a Usable Security Protocol into User Authentication Services Design Process". The focus of this process is to increase understanding between those building authentication systems and the users that they are building for at the beginning of a project, not as an evaluation for the final product. However, it is a unique process focusing on both usable security and authentication. The steps in the process are: define the mission and conceptual design objective, identify the most representative user authentication method categories, develop the Natural Goals, Methods, Selection Language (NGOMSL), develop the authentication risk-assessment matrix, generate the usable security principles from the NGOMSL model, formulate the usable security symmetry inspection method, and demonstrate the usable security symmetry. Based on this process, an usability evaluation can be conducted that is more oriented towards the specific system being evaluated.

Part of the reason that it is so important to look at the usability of biometric authentication in mobile devices and test the usability of it is that users are often unlocking their mobile phones (such as with the iPhone) on average of 80 times a day (Griffin 2016). With so much usage, it is important that users feel they have a secure and usable way to unlock their devices, and if they do not feel that way about biometric authentication, then many will likely continue to use authentication options such as pins, patterns, passwords, or use no authentication at all. For biometric authentication to grow and become more widely used, usability and trust must increase. And because biometric authentication doesn't always have a good UX or is always very usable, it is much easier for people to default to what they have been doing for years. For something to become widely adopted, it needs to enhance what people do, not just be some 'cool' feature. And this is where biometric authentication has overall been unsuccessful; it does not always enhance a person's usage of their device (in this case, we mean the usage of security functions for unlocking a device). And one way that usability, and in turn user experience, can help enhance a person's usage of their mobile phone is by creating a more seamless and invisible authentication experience. When a person types in a pin, they don't think about it; they just do it. Biometric authentication is working it's way to that point, with it becoming easier and faster to use, but it is not widespread yet nor without its bugs.

Usability and biometric security has been researched, however usability and biometric security in mobile devices has not been researched to the same extent. Since we use mobile phones in a different way than we use computers or other systems that require security, the evaluations, methods, and implementations for computers may not fully apply or work for mobile phones. Evaluations and methodologies need to be adapted to fit mobile environments for more accurate representation and analysis. However, fixing the usability of these systems will not fix everything; users must also realize the extent of how important security is and properly understand the risks involved (Sasse 2004). Risks need to be weighed against real-world fixes (Sasse & Flechais 2005).

Nielsen (2000) made an important point when discussing security and human factors, which is "higher security through realistic design". The reason why this is important is that people have often been told, for example, a secure password should be long and have a variety of letters, numbers, and symbols. The reason why people often write down those passwords is that they aren't realistic security measures. With regards to biometric authentication, all methods should be realistic and not require a person to go out of their way to authenticate or require them to do things they wouldn't normally do. Realistic usable and secure biometric authentication in mobile devices seems to be the direction that the mobile industry is moving towards, though if those requirements aren't met, then biometric authentication may likely never become more widespread.

3 Methodology

With an objective of gaining more insight into the perceptions of usability and biometric authentication in mobile phones, two methods were chosen; surveys and interviews. These methods were chosen as they are the best methods for collecting a large sample of data in a relatively short period of time from a variety of user groups. Other methods were considered such as a case study, diary study, design-based research with a prototype, an observation study, and a focus group. However, these methods were dismissed as some of them are more long-term methods, and others could not be completed at this stage due to more information being required and data to be collected before those methods could be used. The survey and interview methods were also chosen due to the fact that previous research in this area has been conducted with these methods, as has been discussed in Chapter 2. Additionally, both qualitative data and quantitative data can be collected with surveys and interviews.

When first planning which methods to use and what research design to follow, an explanatory design approach was chosen (Allen & Komandur 2019). The first phase would consist of the survey, and a second phase would consist of interviews. Three user groups were chosen, consisting of the general population, those working in usability (or related fields), and those working computer security or biometrics. The aim was to find participants in the usability, security, or biometrics fields who submitted the survey to interview for more in-depth analysis. However, this proved to be difficult as only a couple of participants were interested in being interviewed. Instead, for the second phase of the data collection, usability, security, and biometrics companies were contacted to interview.

After the collection and analysis of the interview and survey data, further research was conducted to find relevant guidelines and principles outside of what was discussed in Chapter 2 that could be used in the creation of the guidelines for this thesis. Several methods were used in the creation of the guidelines, including an affinity diagram, the gamestorming method "The 5 Whys", the gamestorming method "Pain-Gain Map", and a basic thematic analysis. These methods were chosen to visually represent all of the guidelines and principles used in the creation of the final guidelines and to ensure that the creation of the guidelines followed the original purpose and goal. After the final guidelines were created, a number of mobile phones were evaluated against the guidelines to determine if the guidelines could be used as an indicator on the usability and security of different mobile phones and their corresponding biometric authentication methods.

3.1 Survey

3.1.1 Purpose

The purpose of the survey was to gain insight into not just the general population's perspectives of usability and biometric authentication in mobile phones, but to also gain insight from people who work in usability, computer security, and biometrics where there has been a lack of research. It is important to get this additional insight, as the people working in these fields are the ones designing and developing biometric authentication systems in mobile phones. With the goal of gaining insight from multiple target groups, a survey is a good method for gathering a large amount of data in a shorter period of time.

3.1.2 Survey design

The survey was comprised of 29 questions. A majority of the questions were developed based on the surveys discussed in the literature review, including Al Abdulwahid et al. (2015), Ahmed (2017), Bhagavatula et al. (2015), Lovisotto et al. (2017), Riley et al. (2008), and Zirjawi et al. (2015). These questions included: demographics (age range, gender, and educational background), knowledge of biometrics, brand of device used, whether or not the participant uses an authentication method for unlocking their device, perceptions of different authentication techniques (convenience, security, and ease of use), and perceptions of biometrics (ease of use and security). These questions focused on obtaining more quantitative data.

The remaining questions were developed based on the structure of the survey created as well as the literature discussed. These questions included: whether or not the participant has worked with people in the usability field and/or the security/biometrics fields, years of experience (if they work in usability, security, or biometrics fields), an estimate on how often the participant unlocks their phone, what is most important regarding unlocking their phone, what biometric traits have been used for authentication, if problems have been experienced when unlocking a phone, and two open-ended questions on why biometric authentication was or was not used by the participant. Based on the research questions established for this thesis, three more questions were added to the end of the survey, which were about if the participant believes that there is a link or trade-off between security or usability, and a question about which statement the participant believes most when it comes to usability and security of mobile phones. At the end of the survey, participants were encouraged to express any additional thoughts they had about usability and biometric security in mobile phones. These questions focused more on obtaining qualitative data than quantitative. All survey questions were worded in a way to reduce bias and influence as much as possible.

The design of the survey itself was also considered. Baxter et al. (2015) discusses how to build a survey in a way to help increase participant understanding and satisfaction with the survey itself. The title was short and written in a way to provide participants with a quick understanding and purpose of the study. Instructions were clearly laid out with contact information according to NSD requirements, the time needed to complete the survey was provided, and details about anonymity and confidentiality were explicitly stated. The survey used a large, sans serif font with captions and subtitles for clarification throughout the survey. A progress bar was displayed at the bottom of the survey and the questions were placed in a specific order to build up to the main questions and to attempt to reduce influencing other questions and answers. The questions were also grouped and placed into sections, and the survey was created in a responsive format so that it could be answered on a variety of devices and screen sizes. All data collected was anonymous with no other identifying information collected. All data was stored on a secure server and only those associated to the study had access.

3.1.3 Identifying user groups and participants

In order to gather data on the perspectives of usability and biometric security in mobile phones, three user groups were identified: the general population, those working in security or biometrics fields, and those working in usability or relevant fields. Most of the research has been conducted on the general population, however it is also important to consider the perspectives of those who could be designing and developing biometric authentication in mobile phones or mobile phones in general. Thus, perspectives from biometric, security, and usability fields is also important.

The survey predominantly used convenience sampling. In order to find participants from the three user groups, multiple methods were used. One method was to create a post on the website LinkedIn which uses more of a convenience sample. Another method geared more towards obtaining participants from usability, security, and biometrics fields in a purposive sample by posting on design and security forums online (such as LinkedIn groups, Facebook groups, and Reddit sub pages) as well as to send an email to design, security, and biometrics companies asking them to share the survey with employees in their company.

3.1.4 Pilot test

A pilot test was conducted for the survey with one participant. The main purpose of the pilot test was to identify any problems with wording, potential misunderstandings, to find potential bias and influence in the survey so that it could be corrected, and to find if clarification would be needed for participants who do not work in the usability, computer security, or biometric fields. During the pilot test, the participant used the think-aloud method and was timed so that the time required to completed the survey could be more accurately estimated.

3.1.5 Data analysis

The data collected in the survey was a mix of qualitative and quantitative data. It was determined that basic statistical analyses would conducted such as mean, average, median, mode, standard deviation, and percentages. Data was also aggregated and looked at by the percentages of each answer that participants provided per question as a whole and by each participant group (security and related fields, usability and related fields, and general population). The data was further analyzed by conducting a correlation analysis between the questions and answers provided.

3.2 Interviews

3.2.1 Purpose

The purpose of the interviews was to go more in-depth from the survey data. Only so much information can be gathered in a survey regarding a specific context with so much explanation that cannot be clarified. The intent was to base the interview questions off of the survey and the literature review to obtain more thorough and well-rounded data. Most of the data collected on the perceptions of usability and security have been in the form of surveys and with the general population, so interviewing those who work in the usability, UX, security, or biometric fields can provide more robust data and a better understanding of if the data collected during this phase aligns with the literature that was found or not. Therefor, interviews are a good method of collecting more in-depth data from multiple sources.

3.2.2 Interview design

Based on the literature review and the survey, a semi-structured interview with eleven questions was created. The interview was broken down into three sections: opening, discussion, and closing, which is based on an idealized interview flow (Baxter et al. 2015). In the introduction section, the questions review some of the data that was collected in the survey such as position, years of experience, devices used, and authentication methods used (if at all). The discussion section then narrowed the focus to perceptions of security authentication in mobile phones, then specifically biometric authentication, the usability of unlocking mobile phones, and whether biometrics are a usable authentication option or not. Then the questions that followed widened in perspective to ask if there is a trade-off between security and usability, if so/not, why, and if mobile phones can be both secure and usable. These questions led to the closing section of the interview, where only one question was asked, which was about how the participant believes that usability and biometric security can be improved in mobile phones. All questions were written and worded in a way to attempt to reduce potential bias, leading words, and influence as much as possible.

All participants were required to sign a consent form before beginning the interview through a PDF that was emailed to them. All consent forms were printed and kept separately from the data collected, and the data did not reference their name, company, or any contact information. The participants were labeled as participant #1, #2, and so on in the data to increase anonymity. The data was collected from the interviews via notes taken by the researcher and were digitized and stored on a secure server. No audio or video recordings were collected. Only those associated with the research study had access to the interview data. The interviews consisted of a purposive but predominantly convenience sample.

3.2.3 Identifying user groups and participants

Initially, the goal for the interviews was to find participants who had already participated and completed the survey for a more explanatory research design. However, after careful consideration and a lack of responses in that fashion, it was decided that participants would be found via another method. Several companies that work with security, biometrics, and usability were identified and contacted via email in an attempt to find one or two people from each company to interview.

3.2.4 Pilot test

Two separate pilot tests were conducted with the interview questions. The purpose of these pilot tests were to test how a usability and a computer security "expert" might react to and understand the questions, to see if there would be any potential misunderstandings, check for potentially leading questions, and to see if any clarification might be needed. Two different pilot tests were conducted to also test the duration of the interview to check if the original estimate of 30-60 minutes was accurate.

3.2.5 Data analysis

The data collected during the interviews was qualitative with all questions written as open-ended questions. Due to the nature of the interviews and the data that was collected, a thematic analysis was conducted to find common themes, beliefs, and differences between the interview participants.

3.3 Guidelines

3.3.1 Purpose

The purpose of the guidelines was to aggregate all of the knowledge and information collected during the background research phase, the interviews, and survey into a set of guidelines that would help in the design and development of more usable security with regards to biometric authentication in mobile phones.

3.3.2 Design

The guidelines for this thesis were designed and created based on 22 sources. Some of the sources used were discussed in the background chapter (Chapter 2), while others were found by using search terms such as information security, computer security, usability, authentication, principles, and guidelines. The sources used in the creation of the guidelines included textbooks on computer security, information security, HCI, and UX design, as well as published research papers, doctoral theses, established guidelines and principles on security, biometrics, and design, and other sources found that were discussed in published books. Sources that were not published in books, research papers, theses, or evidence-based (that could be perceived from the sources found) were not included in the list of sources to be used.

To develop the guidelines, all of the principles and guidelines that were found were aggregated (a total of 220 guidelines and principles from 22 sources). All guidelines were written on sticky notes and an affinity diagram was created to visually compare and group the guidelines to find common categories that could be found and clustered together. Once the affinity diagram was completed, the categories found were documented and a round of further clustering was conducted. Afterwards, multiple "gamestorming" methods were carried out (Gray et al. 2010). One of the methods used is called "The 5 Whys", to ensure that the guidelines at this point and in the next rounds would continue to be edited and focus on the point of the guidelines, which is to attempt to increase security and usability in biometric authentication in mobile phones. Another method that was completed is called the "Pain-Gain Map" whose purpose is to "develop an understanding of motivations and decisions" of the user to ensure that the guidelines take these "pains" and "gains" of authentication into account (Gray et al. 2010).

After the gamestorming methods were completed, the interview and survey data were reviewed and a basic thematic analysis was conducted to find the most common themes discussed so as to find a few points that the guidelines should attempt to follow and fulfill if possible. Following this, the information from the gamestorming methods, the survey and interview data, and the background chapter were reviewed. The guidelines were then re-analyzed using this information, and the final guidelines were created.

3.4 Evaluations

3.4.1 Purpose

The purpose of the evaluation was to assess if the guidelines developed during this thesis could be used as an evaluation method for biometric authentication in mobile phones. The primary purpose of the guidelines developed was to be used as a guide during design and development of biometric authentication in mobile phones for increased usability and security. However, as this was not possible to test during this thesis, it was decided that an evaluation of already implemented biometric authentication methods in several mobile phones would be conducted as a majority of the guidelines developed would still be evaluable after design and development. The evaluation was also used to evaluate the guidelines themselves to discern how much information about a system could be ascertained in regards to both usability and security.

3.4.2 Design

The evaluation form used was created based on the 19 guidelines developed during this thesis. The evaluation form listed the names of all 19 guidelines with a severity rating level (low, medium, high, and critical) and a notes section, similar to that of a heuristic evaluation form. The evaluation form was kept simple as the guidelines are newly developed and can be developed further for refinement. The evaluations were also conducted in a laboratory setting, where the room was set with specific lighting and in a quiet space where the researcher conducted the evaluations in the same manner and sitting position with minimal distractions to help reduce the number of independent variables and outside influences.

To conduct the evaluations, each mobile phone started out with no security settings set. Each phone was evaluated following a number of steps generalized as follows:

1. Phone is set in flight mode
2. Unlock the screen
3. Open settings
4. Open security/authentication settings
5. Set up one biometric authentication trait
6. Lock the screen
7. Use the biometric trait to unlock the screen
8. Repeat for each biometric authentication method allowed on the mobile phone

Each mobile phone and biometric authentication method were evaluated separately following the same steps and criteria, however mobile phones with more than one biometric authentication method were evaluated using the same evaluation form with notes about each biometric trait were specified in the evaluation form.

3.5 Ethical and legal considerations

Before beginning with the methods for this study, the researcher applied for and was granted approval by the Norwegian Center for Research Data (NSD) (Appendix A.1. Before participants partook in the survey or interviews, they were provided with an informed consent form created based on the guidelines set by NSD. The survey consent form was provided before the start of the survey that participants were required to read and had to select "Yes" before the survey could be started. No identifiable personal information or signature was taken for the survey besides age range, field of work, and years of experience. With regards to the interview, a PDF consent form was provided where interviewers were required to sign and provide a date on the form then return it to the researcher via email. All participants were informed that the data collected would remain anonymous and any consent forms with signatures on them would be kept separately from the data to ensure anonymity. The participants were also informed as to who would have access to the data in the consent form. No compensation was provided in return for participation.

4 Results

4.1 Survey

Before beginning the analysis of the survey data, a quick read-through was conducted to scan the survey results for any particularly interesting points or any points of concern. There were three responses that initially seemed a bit concerning when it came to two specific questions. However, upon further analysis of those three responses, it was decided that those responses would be kept as they still provided useful data and information, and the concerning responses did not affect the data in anyway.

The survey was broken up into seven sections, as shown in Table 1. The survey consent form and questionnaire form can be found in Appendix A.2 and A.3.

Section 1	Background information - age, gender, field of work (security, biometrics, usability, related fields, or none of those), biometrics understanding, usability understanding
Section 2	Biometrics or security experience - years of experience, educational background, if they have worked with usability experts, if they own a mobile phone
Section 3	Usability experience - years of experience, educational background, if they have worked with security or biometrics experts, if they own a mobile phone
Section 4	General - educational background, if they have worked with biometrics or security experts, if they have worked with usability experts, if they own a mobile phone
Section 5	Mobile phone usage - how often they unlock their phone, mobile phone brand, authentication method used, importance of phone being secure and easy to use, which authentication method is most secure, convenient, and easy to use, what is most important regarding unlocking their phone, have or do use biometric authentication, what biometric authentication method(s) they have used, if they think biometric authentication is easy to use and secure
Section 6	Biometrics and usability - if they have had problems unlocking their phone, if they use biometrics, why, if they don't use biometrics, why, if they believe that there is a link between security and usability, if they believe that there is a trade-off between usability and security, which statement they most agree with
Section 7	Final thoughts - If they have any other comments about security or biometrics in mobile phones, about unlocking their phone, or authentication

Table 1: Survey sections and questions

Figure 1 shows the breakdown of the age range, gender, and field of work for the survey participants from section one. 49% of participants were between the age of 25-34 years old, 58% of participants were male, and 45% of participants worked in neither usability, security, or related fields. For the rest of this chapter, those who work in usability, UX, UI, or similar fields will be referred to as usability participants, and those working in security, biometrics, or related fields will be referred to as security participants.

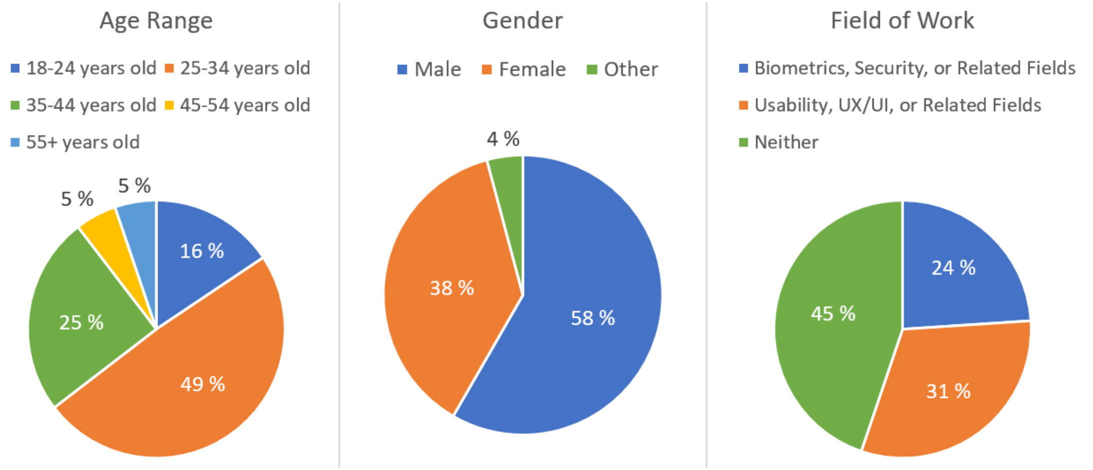


Figure 1: Age, gender, and field of work

When asked about their understanding of biometrics and usability, participants were asked to answer with a score between 1-6, with 1 meaning little to no understanding and 6 meaning an expert understanding. When it came to participants' understanding of biometrics, 35% of participants stated that they had a basic understanding or little to no understanding of biometrics (a score of 1 or 2), 42% of participants had an intermediate or novice understanding of biometrics (a score of 3 or 4), and 23% of participants had an advanced understanding or considered themselves experts in the field (with a score of 5 or 6) (Figure 2).

87% of security participants said that they had a novice to expert understanding of biometrics (a score of 3 or more), with 57% of them saying that they had an advanced or expert understanding of biometrics (a score of 5 or 6) with an average score of 5. 27% of usability participants said they had little to no understanding of biometrics (score of 1 or 2), 60% said that they had a novice to intermediate understanding (a score of 3 or 4), with an average score of 3. 53% of general participants said that they had little to no understanding of biometrics (a score of 1 or 2), and 35% said that they had a novice to intermediate understanding of biometrics (a score of 3 or 4), with an average score of 2. Altogether, there was a decrease in understanding of biometrics from security participants to usability participants to general participants.

39% of security participants said that they had a novice or intermediate understanding of usability (a score of 3 or 4), and 48% said that they had an advanced or expert understanding of usability (5 or 6) with an average score of 4. 30% of usability participants said that they had a novice or intermediate understanding of usability (a score of 3 or 4) and 70% said they had an advanced or expert understanding of usability (a score of 5 or 6) with an average score of 5. 30% of general participants said that they had little to no understanding of usability (a score of 1 or 2), 44% said they had a novice or intermediate understanding of usability (a score of 3 or 4), with an average score of 2. Overall, the median understanding for biometrics and usability were 3 and 4 on a scale of 1-5 respectively.

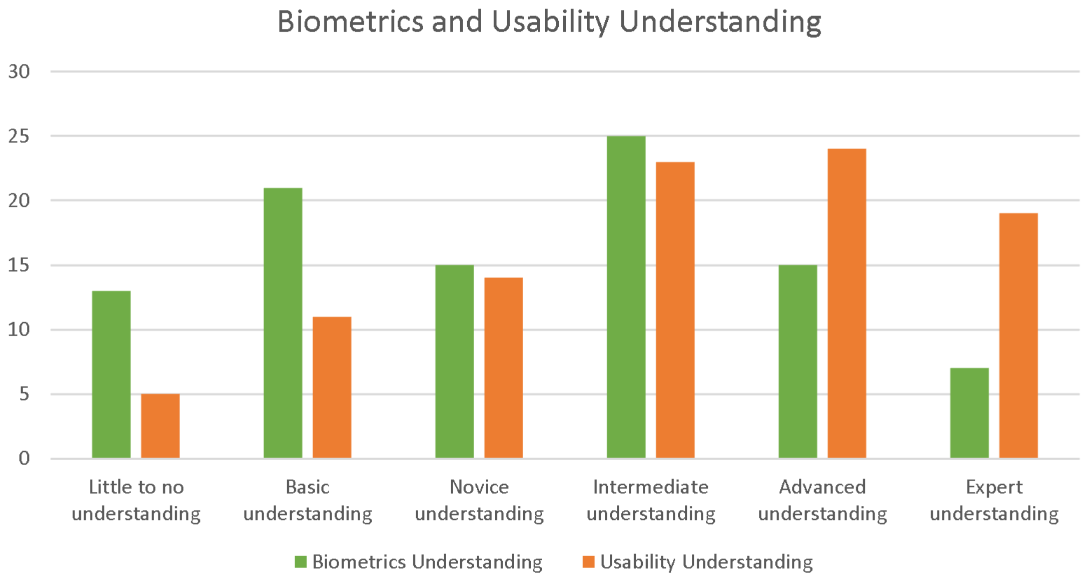


Figure 2: Biometrics and usability understanding

Participants were taken to section two, three, or four based on their response to which field they work in (see table 1 for the questions in those sections). Those who responded to working in computer security, biometrics, or something similar were taken to section two (24% of participants), those who responded to working in usability, UX, or something similar were taken to section three (31% of participants), and those who worked in neither of those fields were taken to section four (45% of participants). In sections two, three, and four combined, 40% of participants have a bachelor's degree, and 44% had a master's degree, and 7% had a doctorate. 63% of usability participants had a master's degree. 83% of security participants said that they have worked with usability experts, 33% of usability participants said that they have worked with security experts, and 19% and 28% of general participants said that they have worked with security experts or usability experts respectively.

After responding to either section two, three, or four, all participants were redirected to sections five through seven. In section five, when asked about how many times the participants unlock their phones, where 26% said that the unlock their phones less than 20 times a day, sometimes only a few times a week whereas 74% said they unlock their phones 20-50 times a day to 50+ times a day. When asked about the brand of mobile phone they use, 56% of participants said Apple, 22% said Samsung, and the remaining 12% use another brand (Huawei, LG, Google, Nokia, Xiaomi, Sony, or Blackberry). 76% of participants use biometric authentication currently, 20% use a traditional password, pin, or pattern, and 4% use no authentication at all. A majority of participants (51%) use fingerprint authentication. About 75% of those participants were users of a well-known brand and the remaining 25% use fingerprint authentication with another phone brand. When asked how important it is that their phone is secure, participants were asked to rate the importance on a Likert scale of 1-5. 7% answered with a 1 or 2, 15% answered with a score of 3, and 78% answered with a 4 or 5, with 50% of those participants providing a score of 5. 87% of security participants provided a score of 4 or 5. When asked how important it is that a phone is easy to use also on a Likert scale of 1-5, 5% said 1 or 2, 7% said 3, and 88% said 4 or 5 with 58% of those participants providing a score of 5. The average scores for both questions were 5. 93% of usability participants provided a score of 4 or 5 on how important it is that a phone is easy to use (Figure 3).

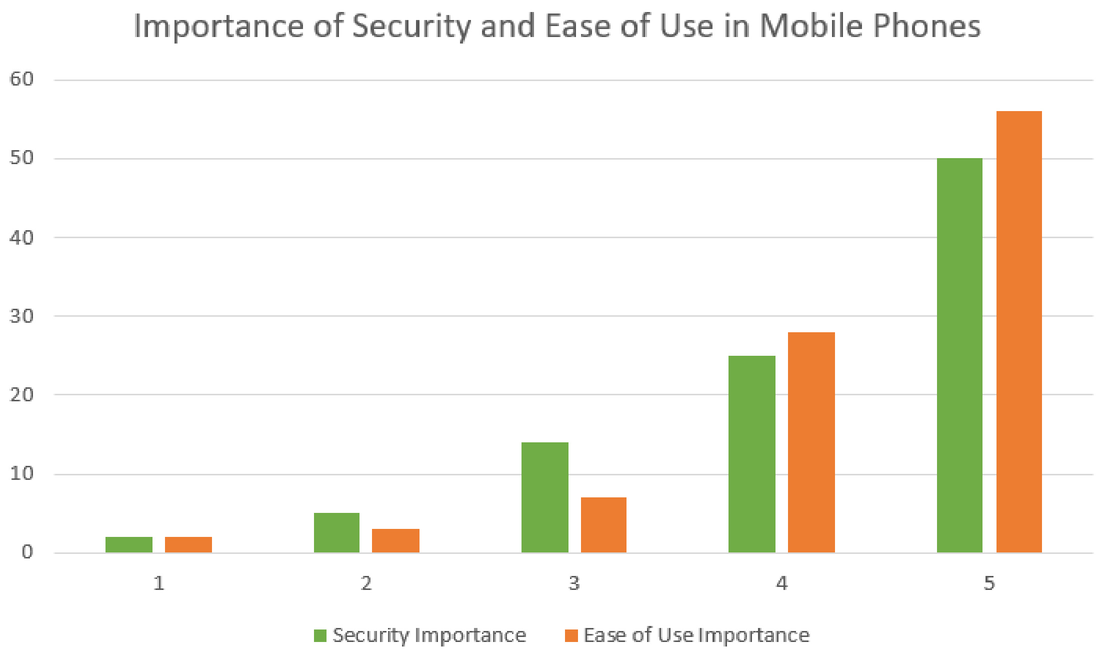


Figure 3: The importance of a mobile phone being secure and easy to use

Participants were then asked which authentication method was most secure, convenient, and easy to use. For the purpose of this survey, convenient and ease of use were separated into two questions, where convenience focused a bit more on time and access whereas ease of use focused on comfort and level of effort. When asked which authentication method participants believe to be most secure, 76% chose fingerprint, face, iris, or biometrics in general and 22% said passwords, pins, and patterns. 83% of security participants chose some form of biometrics. When asked which authentication method is most convenient, 78% said some form of biometrics or biometrics in general, 19% said a traditional method (password, pin, pattern), and 2% said none. 91% of security participants chose some form of biometrics, 87% of usability participants chose some form of biometrics, and only 65% of general participants chose similarly. Broken down, biometrics were chosen as the most convenient method (46% said fingerprints, 17% said face, 12% said biometrics in general), and pins received 10% of responses. When asked about ease of use, 76% said biometrics, 20% said a traditional method, and 3% said none. 83% of security participants, 90% of usability participants, and 63% of general participants chose biometrics as the easiest to use authentication method. When asked which method is the easiest to use, 42% chose finger recognition, 20% chose facial recognition, and 10% chose biometrics overall, with pins and patterns receiving 10% and 9% of responses respectively.

When asked what is most important to participants regarding unlocking their phones, they were able to choose several options, which included "It’s easy", "It’s fast", "It’s secure or safe", "It’s reliable", and "Other". The "It’s fast" option was chosen by 59% of participants, followed by "It’s secure or safe" with 48% of participants, "It’s easy" with 39% of participants, and "It’s reliable" with 39% of participants (Figure 4). In this question, one participant decided to choose the "Other" option as well and described how one time they were in an accident and were in shock, and they struggled to call 911 because they could not authenticate, so that it is important that people are still able to use their phones when in shock, intoxicated, or in another state in which they cannot function as normal.

When asked if participants have used biometric authentication before, 79% said yes, and only 21% said that they have not used or currently do not use biometrics. When asking what biometrics specifically participants have used, 74% said they have used fingerprint (87% of security participants have used fingerprint), 45% said that they have used face or iris (78% of security participants, 40% of usability participants, and 30% of general participants have used face and/or iris), 16% said that they have used gait, signature, voice, or keystroke, and 16% have never used biometrics. 5% of participants have used biometrics in the past but currently do not use them. When asked if participants believe that biometrics are easy to use, 63% of participants said yes, 5% said no, 19% said it depends. When asked if they think biometrics are secure, 67% said yes, 8% said no, 23% said it depends, and only 2% chose to instead mark that they have not used biometrics before, so even though some others have not used biometrics before, they chose to answer if they thought biometrics were secure or not.

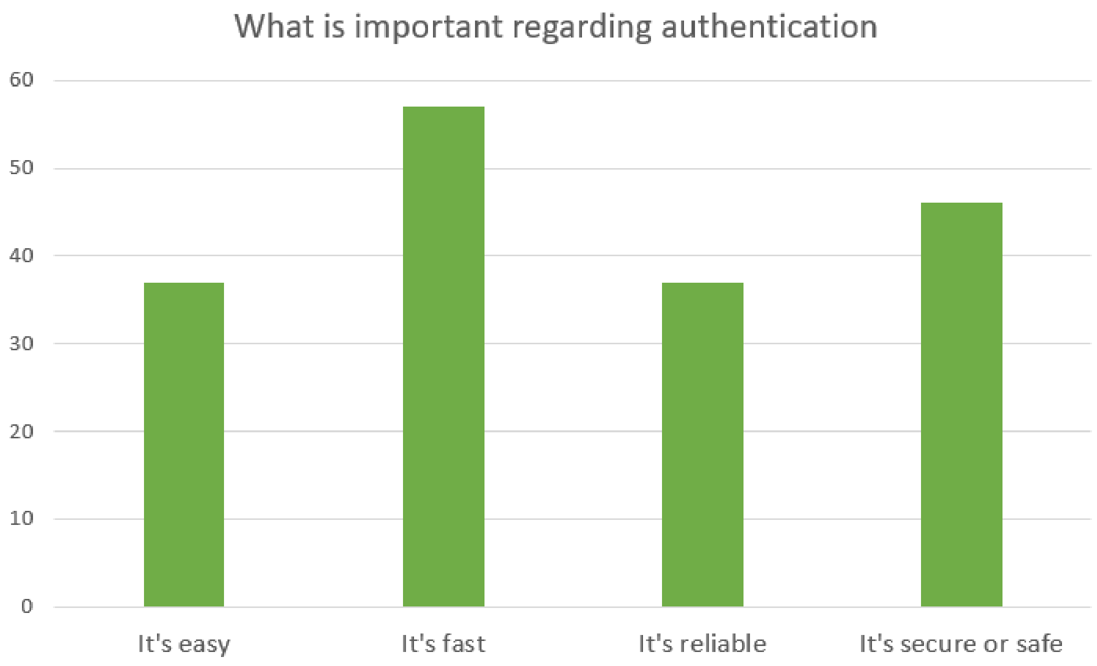


Figure 4: The importance of a mobile phone being easy, fast, reliable, and secure to use

In section six, one of the questions asked if participants have had issues with unlocking their phones. 25% of participants said they have not had issues with unlocking their phones, whereas 75% said that they have (87% of usability participants said yes). 50% said yes they have had issues with fingerprint, followed by 23% had issues with face, 19% with pin, 17% with password, 2% with iris, and 3% with other biometrics.

For the question about if participants use biometrics, why, common answers included convenience, speed, ease, reliability, and the feeling of it being secure. Some participants commented that biometrics are harder to "break" than traditional methods, it is "fun", and requires fewer touches and movement than other methods. Others said biometrics are "trendy" or that they are confident that only they can unlock their phone. One participant mentioned how before biometrics were in mobile phones, they did not use any authentication method because it was "too slow and cumbersome to enter a pin or a pattern". A few other participants mentioned a higher level of convenience and security than a pin or that "it’s secure [on a particularly well-known brand of mobile phones] and faster than entering a code". One participant mentioned how they can set up multiple fingerprints and that they "set up fingerprint on my kids’ phones and [tablets] so I don’t need to know their passwords". And couple participants mentioned pay options through their phone brand, that there is a higher level of difficulty for others to obtain their biometric trait to unlock their phone, and that with biometrics they don’t have to worry about forgetting their password.

For those who don't use biometrics or have stopped using biometrics, common answers included not having the option on their phone, being used to traditional methods, or concerns/-experiences with a high failure rate with biometrics. Some participants mentioned how they do not want any devices that they "use regularly to store this kind of information", the "high rate of false negatives" (FRR) in general or with voice recognition, and concern about how others could force unlock it using the users finger(s). Another participant simple stated "it has faults", and another participant said that they don't give their phone away so no security is needed. Other participants mentioned not liking the placement of fingerprint sensors as a reason for not using biometrics and that other methods are more convenient when a phone is on a table for example. Some participants said that other authentication methods are more convenient than biometrics and that biometrics are not the default on their phone. Another said that their pin is muscle memory now or that they are used to one method and just did not bother to change methods. One participant discussed the difficulty in situations of high stress or inebriation as a reason for no longer using biometrics.

The next two questions asked participants if they believed if there was a link between usability and security, and if they believe that there is a trade-off between the two. 76% of participants believe that there is a link between security and usability with 14% not sure and 10% saying no. 95% of security participants, 80% of usability participants, and 63% of general participants said that yes there is a link between security and usability. 28% of general participants were not sure. 52% of participants believe that there is a trade-off between security and usability with 23% said maybe, not sure, and 23% said no there is not a trade-off. 68% of security participants said that there is a trade-off, and 37% of general participants were not sure.

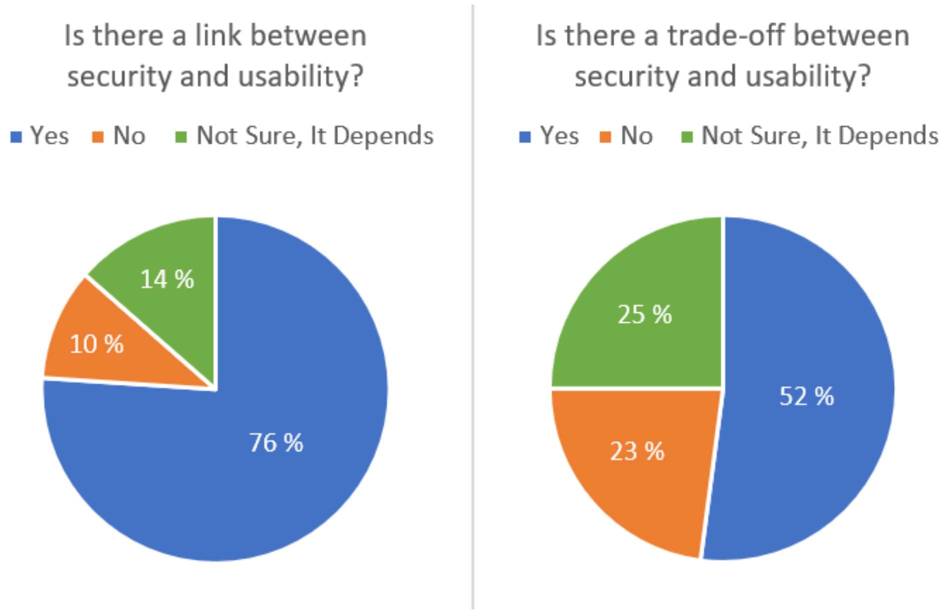


Figure 5: Link and trade-off between security and usability

The final question in section six was a list of statements where participants had to choose which they most believe. 63% of participants selected the statement: "A phone can be both easy to unlock and secure (but they aren't always like this right now) (70% of security participants chose this statement), 15% selected the statement: "Phones are both easy to unlock and secure", 11% selected the statement: "A phone that is easy to use is less secure, and phones that are more secure is not easy to use", and 11% selected the statement: "I mainly care about how easy a phone is to use" or the statement: "I mainly care about if a phone is secure to use".

In the final section (section seven), there was only one question which was optional. The question asked if the participants had any other thoughts or comments about the topics discussed. One participant said that "most biometrics have issues with checking if the person is alive or not; a password might have an edge there". Another participant mentioned how if a password is stolen, it can be changed, and that even though biometrics may be the easiest method of unlocking a phone, they are not sure about how secure it is. Some participants were saying that as technology continues to develop, biometrics will be less secure and more advanced features will be needed or that the idea of biometrics is brilliant but the technology needs improvement. Another comment mentioned how most phones use small fingerprint scanners which reduces the security level, so cameras may be more effective for capturing fingerprints or faces for authentication. Another participant discussed fingerprint scanners and how sensors on the back of phones has a negative impact on usability. A different participant said how security needs to be seamless and convenient or users will bypass it for more ease of use. One participant wrote about how if biometric authentication could be easy and intuitive for all ages and secure enough that governments and others could not hack them, then all working in this area could go to other fields, but as of now there is a strong trade-off between security and usability. They believe it will take another five years before this problem is fixed in phones. One participant discussed how good implementations should be seamless, secure, and fast and how bad implementations should not happen because they create annoyance. They went further to say that biometrics should eventually be completely in the background without users having to think about it, so that if it is the genuine user you have access, otherwise not. Another said that maybe biometrics are easier to use, but they have less security.

One participant said that they believe their phone is secure enough and that even though it is possible for someone to get their fingerprint, it seems like more work than is worth it. Another participant disagreed by simply stating that if someone wants it enough, they can get it (meaning that if someone really wants to get into their device and they use biometrics, they can get access). A few of participants mentioned how they like fingerprint, however it can be very inconvenient when their fingers are wet, messy, or while cooking. One participant made a comment about how face recognition doesn't always work when they are not wearing their glasses, which is a common problem now with face recognition. Another person mentioned how they don't like how passive face recognition is with concern that when they sleep someone could open it just by pointing it at their face, but they like how intentional fingerprint is and how reliable and convenient face recognition is. One participant made a comment about how biometrics that they prefer are not available for them to use. Another uses iris and mentioned issues with iris scanning when wearing glasses. One other participant said that it seems like it's harder to make sure that a camera captures their face or eye than it is to place a finger on a sensor. A participant said the strongest and at the same time weakest point in biometrics is that they are unique and that it is unique forever; it can't be easily changed. On another note, another participant said that biometric sign-in will become universal across all platforms in the future. Another said that in their experience when biometrics don't work it is usually user error. One of the last comments was about how siblings may be able to unlock each other's phones with face recognition, but when the technology "get[s] more intelligent" they would prefer face recognition, that iris has a ways to go before it is convenient, and that fingerprint doesn't work every time.

4.1.1 Correlation analysis

A correlation analysis was conducted on the survey data for further analysis. A majority of participants ages 35-44 use biometrics (90%) as well as having a highly favorable view of biometrics when it comes to security (85% said biometrics are the most secure method), convenience (100% said biometrics are the most convenient method), and ease of use (85% said biometrics are the easiest method to use). A majority of these participants also believe that there is a link between usability and security (91%). Participants over the age of 45 also had a highly favorable view of biometrics, with 100% of participants saying that biometrics is the most secure and easy to use authentication method, and 90% saying biometrics are the most convenient method. 100% of these participants also currently use biometric authentication. 83% of male participants believe that there is a link between security and usability as well as currently use biometric authentication. 91% of male participants have used biometrics, and a majority of male participants believed biometrics to be the most secure (73%), convenient (86%), and easy to use (82%) authentication method.

There was correlation between participants who use a particularly well-known phone brand and the authentication methods that they use, where 94% of the users of that phone brand use either fingerprint or face recognition. Also, 94% of those participants and 95% of another well-known phone brand user participants provided a score of 3, 4, or 5 on the importance of a phone being easy to unlock. Overall, there was a high correlation between the particularly well-known phone brand users and favorable perceptions of biometrics. Another correlation was between understandings of biometrics and usability and a link between the two. As the understanding of biometrics and usability increased, so did the belief of a link between security and usability as well as the use of biometric authentication. In other words, when participants had a higher understanding of biometrics or usability, there was a greater chance that those participants believed that there was a link between usability and security.

4.2 Interviews

Six interviews were conducted after the survey was completed (see Appendix A.4 and A.5. Those interviewed came from a variety of fields, with job titles such as UX Designer, Design Technologist, Developer, and IT/System Developer. They have a range of experience in their respective fields, from six months to thirty-three years. Five of the participants currently use some form of biometrics to unlock their phones.

One of the first questions interview participants were asked was about their thoughts of current security measures for unlocking mobile phones. Some participants discussed how some security measures are likely to be excessive for most users and not practical. There was also discussion around biometrics specifically, that biometrics has "reached maturity" and is overall more secure than traditional methods, but there are still weaknesses. There was concern about how data and templates are stored for biometric authentication, and that the sensitivity of information in mobile phones now makes authentication more important. One participant discussed in detail about how the person who wrote the original report on how to create safe passwords apologized in 2006 for creating the "best practices" for passwords and how passwords are not safe.

Another question asked built off of the previous one, asking what participants thought specifically about biometric authentication. Participants discussed not locking users into specific security measures or authentication methods, and how they should be able to use multiple different biometric authentication methods. There was also discussion around how biometric information is stored and sent, and how margin of error is very important for biometric authentication. One thing that interview participants mentioned that they liked about biometrics is that people don’t really have to think about unlocking their phone with biometrics, but with traditional methods they do.

The following question asked was about usability in the authentication process of unlocking phones and if it is important or not. There was discussion about how if authentication can be disabled or a less secure authentication method will be used if the methods have a high failure rate or are not usable. Memory is not an issue with biometrics which can make it a more usable method since biometrics are about the actual person. Participants also discussed 2-factor authentication and how it is a more secure authentication method, but that it might be overboard for mobile phones.

The next question also tied in with the previous question which was about if biometrics are a usable option or not. Participants discussed how the usability of biometrics depends on the use case, and when biometric authentication is working well it is safer and quicker than traditional methods. If very important information is on a device then regular authentication methods should not/would not be used, but for day-to-day usage then biometrics are very convenient. Participants also discussed how a lot depends on the resources for protecting information on a device and consistency to see if it is usable or not.

Then there was a question about if the participants think there is a trade-off between usability and security. Some participants said that there is a trade-off, however that it is not necessarily a bad thing. Most people are dependent on consistent and easy to use things, so there needs to be a balance. Another participant said that there is a trade-off due to poor implementation. Participants discussed having a balance between usability and security and providing explanations to users about what is going on and how things work. The real risks need to be looked at, and this is why independent testing is so important. If you leverage too much security then people will take shortcuts and circumvent security to make things easier.

Following that, participants were asked if they believe that mobile phones can be both secure as well as usable. Participants discussed how the definition of security is important to answer that question. At the moment we aren't too advanced, but still are able to create good solutions. Security always needs to be in the back of the mind and for most practical purposes it is reasonable to see some risks. When it comes down to it, high security can be achieved, but at a cost. Several participants discussed how we are already at the point of having secure and usable phones, or at least the technology is there for it. It's all about how the technology is used and the security is implemented.

The last question asked was the most weighty and also the most challenging question. It asked participants to think about how security and usability could be improved in mobile phones. Participants discussed how it goes back to how theoretically there can definitely be more usability and security in mobile phones, but in practice it hasn't really been that way. Biometrics are theoretically unique, but there needs to be an improvement in biometric authentication for it to be a more safe and secure authentication method. It also depends on what effort people are willing to make for their security. Participants also discussed how people are either informed or not, and that affects security and usability a great deal. They also talked about how phones tell us that we can use a backup method for more security, but the backup methods provided are not usually secure methods. A couple participants discussed how they believe that UX experts should be a part of development in cross-functional teams and how the design of the phone itself needs to be considered. Everything goes back to the users.

4.2.1 Thematic analysis

One of the common themes that emerged during the thematic analysis for the interviews was regarding the users of mobile phones. A few of the participants talked about how it all "goes back to the user" and how things often depend on the specific person as well. Participants also discussed that mobile phone users should not be forced to use or do something specifically or forced to not use something else. If users don't like something, they will just disable or find ways to circumvent their mobile phones' security measures. Several participants discussed how users, especially users from older generations, would likely want more consistency, which is one reason that a great deal of people use the same password or pin for multiple accounts or purposes "as their default method because they are used to it". There was also discussion about what users and potential users are willing to do or how much effort they are willing to put in to security measures that they use. It is important to keep in mind what is "practical for the end user". One participant said "most people are dependent on easy to use things", and another said "[users] are either informed or not".

A second theme that became apparent from the thematic analysis was surrounding weaknesses in security measures in mobile phones. Several participants brought up Type I and Type II errors and margins of error, and there was also discussion around how the biometric information and templates are sent and stored for the authentication process. There was also discussion around "back doors" in software, caused by software quality and resources that have been assigned to the design and implementation of security. One participant discussed how "theoretically it can work and [security] can increase, but in practice it hasn't been that way". Another participant also discussed how backup methods make users think that they are being more secure with heightened security, but "the methods used as a backup aren't secure methods". When it comes to challenges with regards to security and authentication in mobile phones, participants said that it is "hard to define a bullet-proof system" and that "no security is foolproof".

Five of the six interview participants discussed how a balance between usability and security needs to be found when they were asked about there being a trade-off between usability and security or not. Several participants discussed how there is a fine line between the two, or how in general there's a trade-off between security and usability but that doesn't mean that it is a problem. Several participants also discussed 2-factor authentication and how it provides heightened security, however a couple of participants pointed out how that might be excessive for mobile phones or not practical in this specific use case.

Throughout the interviews, there were a few comments that participants said that had a bit more emphasis placed on them. "Usability is the reason why biometrics are used", and "authentication needs to just work". "UX should not interrupt security" and that "there needs to be an explanation to the user". A couple more comments were about how "independent testing is so important", "there needs to be a way to protect the device even when there is no physical access to it", and "there is always a question about what is the best option today".

4.3 Guidelines

A list of previously established guidelines and principles was created. A total of 22 guidelines, principles, books, papers, etc. were utilized. An overview of the sources are shown in Table 2 - 5.

Author	Source	Guidelines/Principles
Saltzer & Schroeder (1975)	The Protection of Information in Computer Systems	Economy of mechanism, fail-safe defaults, complete mediation, open design, separation of privilege, least privilege, least common mechanism, psychological acceptability
Nielsen (1994)	10 Usability Heuristics for User Interface Design	Visibility of system status, match between system and real world, user control and freedom, consistency and standards, error prevention, recognition rather than recall, flexibility and efficiency of use, aesthetic and minimalist design, help users recognize/diagnose/recover from errors, help and documentation
Yee (2002)	User Interaction Design for Secure Systems	Path of least resistance, appropriate boundaries, explicit authorization, visibility, revocability, expected ability, trusted path, identifiability, expressiveness, clarity
Johnston et al. (2003)	Security and Human Computer Interfaces	Convey features, visibility of system status, learnability, aesthetic and minimalist design, errors, satisfaction, trust
Lockwood & Constantine (2003)	Usability by Inspection: Collaborative Techniques for Software and Web Applications	Visibility, feedback, structure, reuse, tolerance, simplicity
Dix (2004)	Human-Computer Interaction	Predictability, synthesizability, familiarity, generalizability, consistency, dialog initiative, multi-threading, task migratability, substitutivity, customizability, observability, recoverability, responsiveness, task conformance
Shneiderman & Plaisant (2005)	Designing the User Interface	Strive for consistency, design for plasticity, offer informative feedback, design dialogues to yield closure, prevent errors, permit easy reversal of actions, support internal locus of control, reduce short-term memory load
Garfinkel (2005)	Design Principles and Patterns for Computer Systems That Are Simultaneously ...	The principle of least surprise, good security now (don't wait for perfect), provide standardized security policies, consistent meaningful vocabulary, consistent controls and placement, no external burden

Table 2: Sources used for the creation of guidelines part 1

Author	Source	Guidelines/Principles
Yee (2005)	Guidelines and Strategies for Secure Interaction Design	Match the most comfortable way to do tasks with the least granting of authority, grant authority to others in accordance with user actions indicating consent, offer the user ways to reduce others' authority to access the user's resources, maintain accurate awareness of other's authority as relevant to user decisions, maintain accurate awareness of the user's own authority to access resources, protect the user's channels to agents that manipulate authority on the user's behalf, enable the user to express safe security policies in terms that fit the user's task, draw distinctions among objects and actions along boundaries relevant to the task, present objects/actions using distinguishable, truthful appearances, indicate clearly consequences of decisions the user is expected to make
Yong Gu et al. (2006)	A Usability Checklist for the Usability Evaluation of Mobile Phone User Interface	Predictability, learnability, structure principle, consistency, memorability, familiarity, recognition, visibility, simplicity, substitutivity, feedback, error indication, synthesizability, responsiveness, recoverability, flexibility, user control, customizability, effectiveness, efficiency, effort
Ibrahim et al. (2010)	Assessing the Usability of End-User Security Software	Interfaces design matches the user's mental model, aesthetic and minimalist design, visibility of the alert detector name, establish standard colors to attract user attention, use icons and visual indicators, explicit words to classify the security risk level, consistent and meaningful vocabulary and terminology, consistent controls and placement, learnability/flexibility/efficiency of use, take advantage of previous security decisions, online security policy configuration, confirm/recover the impact of user decisions, awareness of system status at all times, help prevention and remote technical support, offer responses that match user expectations
Hess (2010)	20 Guiding Principles for Experience Design	Stay out of people's way, present few choices, limit distractions, group related objects near each other, create a visual hierarchy that matches the user's needs, provide strong information scent, provide signposts and cues, provide context, avoid jargon, make things efficient, use appropriate defaults, use constraints appropriately, make actions reversible, reduce latency, provide feedback, use emotion, less is more, be consistent, make a good first impression, be credible and trustworthy

Table 3: Sources used for the creation of guidelines part 2

Author	Source	Guidelines/Principles
Labati et al. (2012)	Biometric Privacy Protection: Guidelines and Technologies	The scope and capabilities of the system should be declared to the user and should not be extended during the life of the system, user control and personal data (voluntary), disclosure/auditing/accountability of the biometric system, data protection techniques
Nielsen (2012)	Usability 101: Introduction to Usability	Learnability, efficiency, memorability, errors, satisfaction
Norman (2013)	The Design of Everyday Things	Discoverability, feedback, conceptual model, affordances, signifiers, mappings, constraints AND use both knowledge in the world and knowledge in the head, simplify the structure of tasks, make things visible, get mappings right, exploit the power of constraints, design for error, when all else fails, standardize
Peisert et al. (2013)	Principles of Authentication	Identity should be verified as long and as frequently as access to a resource is permitted; if access is ongoing then identity verification should be continuous, authentication is about validating whether or not someone is who they claim to be and about determining whether that person intends to authenticate and is not being coerced (for example), computers should provide measures of confidence to humans and those humans should ultimately make authentication decisions (not computers), authentication should be trivial for the person legitimately authenticating but hard for an adversary to defeat
FIDO Alliance (2014)	FIDO Privacy Principles	Require explicitly informed user consent for any operation using personal data, provide clear context to the user for an operation, limit collection of personal data, use personal data only for operations, prevent identification of a user outside of operations, biometric data must never leave the user's personal computing environment, protect data from unauthorized access or disclosure, allow users to easily view and manage their authenticators

Table 4: Sources used for the creation of guidelines part 3

Author	Source	Guidelines/Principles
Merkow & Breithaupt (2014)	Information Security: Principles and Practices	There's no such thing as absolute security, the three security goals are confidentiality/integrity/availability, defense in depth as a strategy, when left on their own people tend to make the worst security decisions, computer security depends on functional & assurance requirements, security through obscurity is not an answer, security = risk management, three types of security controls are preventative/detective/responsive, complexity is the enemy of security, fear/uncertainty/doubt don't work in selling security, people/process/technology are all needed to adequately secure a system, open disclosure of vulnerabilities is good for security
Preece et al. (2015)	Interaction Design: Beyond Human-Computer Interaction	Effectiveness, efficiency, safety, utility, learnability, memorability
Stallings & Brown (2015)	Computer Security: Principles and Practice	Economy of mechanism, fail-safe defaults, complete mediation, open design, separation of privilege, least privilege, least common mechanism, psychological acceptability, isolation, encapsulation, modularity, layering, least astonishment
Biometrics Institute (2017)	Biometrics Privacy Guidelines	Respect for individuals privacy, proportionality, informed consent, truth and accuracy in business operations, protection of biometric data collected, complaints and enquiries, purpose, non-discrimination, accountability, sharing of biometric data, provision of advance warnings of surveillance, transmission of biometric data beyond national boundaries, employee biometric data must be protected, limit the extent of personal data exchanged and retained, maintain a strong privacy environment, maintain privacy logs
Sons et al. (2017)	Security from First Principles	Comprehensivity, opportunity, rigor, minimization, compartmentation, fault tolerance, proportionality

Table 5: Sources used for the creation of guidelines part 4

4.3.1 Guideline creation methods

After all guidelines and their subsequent descriptions were listed (a total of 220 guidelines and principles), each guideline was written on a sticky note and an affinity diagram was created (Figure 6). With an affinity diagram, the guidelines could be shown more visually and combined into categories based on name and description of the guideline more easily.

Figure 6: Affinity diagram

Based on the affinity diagram, 29 categories were created without labels, including one "Other" category. After the 29 categories were written down with their subsequent descriptions, the guidelines were again analyzed, combined, and reduced to 21 categories, with one additional "Other" category (a total of 22 categories). Subsequently, the guidelines that had previously been placed in the "Other" category were then analyzed and placed in one of the 21 categories created that they could befit (Table 6). The 21 categories were then initially labeled:

Visibility and discoverability	Help and errors	Learnability
Security, authentication, and privilege	Psychological acceptability	Trust
Structure and comprehensivity	Defaults	Clarity
Flexibility, customizability, and simplicity	Defense in depth	Mappings
Effectiveness and constraints	Authority/Authorization	Isolation
Efficiency and responsiveness	Feedback	Consistency
Open and minimalist design	User control and consent	Privacy

Table 6: Guidelines draft category labels

Following this, a few "gamestorming games", or methods, were conducted to maintain focus on the goal of the guidelines as well as to maintain focus on the users. One of the games conducted was "The 5 Whys". The purpose of this game is "about seeing the bigger picture or relating a problem to its context" (Gray et al. 2010). The result of this was:

What is the purpose of these guidelines?

1. To increase usability and security, specifically biometric authentication in mobile phone. Why?
2. Because there is often a trade-off between usability and security in mobile phone authentication. Why?
3. Because people often want something that is convenient and easy to do but they still want some form of security. Why?
4. Because they want to protect themselves and have privacy but not in a way that impedes their daily life. Why?
5. Because they don't want their information/ things stolen or used without their permission. Why?
6. Because people want control and privacy.

The next gamestorming method used is called the "Pain-Gain Map". This method was used to check and ensure that the guidelines at this stage and in the following stages would maintain a focus on the users. This method focused on figuring out the current pains that users have with regards to authentication on mobile phones and current gains that they have in the same context. The results of this method is shown in Table 7.

Pains	**Gains**
Takes time	Can be easy or fast
Have to remember to do something	Provides a level of security
One (or several) extra steps	Increases privacy
Not as easy as doing nothing	Confidentiality
Not always accessible	Social norm
Creates a single point of failure	Simple set-up
Can get locked out	Non-intrusive

Table 7: Pain-Gain Map for authentication

The "pains" describe how using an authentication method "takes time", whereas using no authentication method does not take time. Another listed "pain" was that users "have to remember to do something" such as input a pin, enroll their finger on a specific sensor in a specific way, et cetera. Authentication can also take one (or several) steps to complete so that a user can access a phone, and it is easier to do nothing. Authentication is not always accessible as well, and that if accounts are logged in to on a mobile phone and the authentication method is known by another party, it creates a risk. A user can also run the risk of getting locked out of their device. The "gains" describe how some authentication methods can be easy and/or fast to use (though not all). Using a form of authentication also provides a level of security and can increase privacy and confidentiality. Also, another "gain" is that it is a social norm to use an authentication method. It can also be said that it is a "gain" that there can be a simple set-up so that it doesn't take much effort or time to configure, and are often non-intrusive.

After completing the gamestorming methods, the survey and interview data as well as the background from Chapter 2 was reviewed. Based on this information, a few common themes emerged. These themes included:

1. Communication
2. Satisfaction and trust
3. Simplicity and convenience
4. Privacy
5. Accessibility

Based on the gamestorming methods conducted and the themes found, the 21 guidelines were reviewed and re-analyzed.

4.3.2 Final guidelines

A final total of 19 guidelines were created and revised. These guidelines are based on the initial 22 sets of guidelines and principles that were found and are based on research (dating from 1975-2017), data collected from the interviews and survey discussed in Chapter 3 and 4, the background information discussed in Chapter 2, and the common themes found from the data and background information. The final guidelines are as follows:

1. Visibility and discoverability
2. Clarity
3. Trust
4. User control and consent
5. Open and minimalist design
6. Psychological acceptability
7. Consistency
8. Feedback
9. Errors and help
10. Effectiveness and constraints
11. Efficiency
12. Learnability
13. Defense in depth
14. Authority and privilege
15. Privacy
16. Mappings
17. Security and authentication
18. Flexibility, customizability, and accessibility
19. Isolation

Two guidelines were not removed, however the guidelines were rearranged for increased clarity and to reduce potential redundancy. Security, authentication, and privilege was changed to security and authentication, and privilege was removed from this category and combined with authority. Structure and comprehensivity where split up, where structure was combined with efficiency (as better structure can increase efficiency) and comprehensivity was combined with trust (because increased comprehension can lead to more trust). Defaults was combined with efficiency as creating defaults can increase or decrease efficiency depending on implementation. Flexibility, customizability, and simplicity was changed to flexibility, customizability, and accessibility. Simplicity was removed and combined with open and minimalist design. And finally, efficiency and responsiveness was simplified to just efficiency.

4.3.3 Final guidelines explanation

To better understand each guideline, an explanation of each one is as follows:

1. Visibility and discoverability
   Creating systems that allow users to easily determine what actions are possible, what the current state of the device is, provides a strong information scent via clear language and expectations, provides signifiers, signposts, and cues so that users do not get lost, clearly communicate feedback, reduce latency so that if users must wait, they know that the system is working and why, not obscuring information or pathways, always keeping users informed, making the security status visible, allowing information and authority to be easily reviewed, making all aspects of a task available and apparent when needed, and overall every aspect, its purpose, reason for being shown (or hidden), and its existence should be clear.
2. Clarity
   Clearly showing the expected ability of the system so that the user does not think that something is possible that isn't or that something isn't possible when it is, information about numerical values should be easily understandable to the user, features are clearly conveyed with related objects and aspects placed near each other, objects and actions are clearly distinguishable and identifiable with their truthful appearances, all effects of security actions are clearly apparent before and after action is taken, there is clear context and reasoning for all operations (affordances), context is always apparent, distractions are limited, meaningful descriptions of policies and allowing users to express policies in terms that fit with their goals, identifiability regarding actions and representations, offer responses that match the users expectations, and create appropriate boundaries where the interface exposes and enforces distinctions between object and actions in ways that matter to the user.
3. Trust
   Providing accountability for the system, having open disclosure and auditing of the purpose, data, vulnerabilities, and how the system works, identifying and accounting for all relevant systems and related risks in a system, creating an air of trustworthiness, increasing understanding to build trust, truth and accuracy in the system and business with efficacy and reliability, reducing fear and uncertainty, showing respect for user data and privacy, preventing identification outside of operations, using a trusted path for communication between the user and entity trusted with data and authorities, apparent and clear scope and capabilities, storing only the minimum amount of information necessary for performance, and increasing satisfaction of use and design of the system.
4. User control and consent
   Supporting the internal locus of control that users have, providing confirmation and recoverability of user decisions, clearly indicating consequences of decisions and actions (all aspects are explained, the implications, and reflects what the user intends), providing control

and freedom to users about what functions can be used with undo and redo, using emotion to aid in decisions and create a more enjoyable experience, recoverability and reversibility to aid in control, requiring and showing explicit informed consent for all operations that have an impact on the user and/or their data (who is collecting the information, why, who has access, how it is stored, access rules, how it can be deleted), task conformance, and remembering that users need help to make good security decisions.

5. Open and minimalist design
   Creating a design that is open and not secretive, creating a visual hierarchy that matches the user's needs, developing a system where everything that is used and shown has a purpose (less is more), minimizing the size, quantity, and complexity of a system, providing freedom from artificial constraints of input dialog imposed on the system, allowing users the ability to evaluate the system, and providing an aesthetic and minimalist design where only relevant information and security aspects are displayed in a clear, simple, and pleasant way.
6. Psychological acceptability
   Little surprise where the system acts in accordance with user expectations, always responding in a way that is least likely to astonish a user, staying out of user's ways (no obstacles or interruptions), and the system should be designed for ease of use where protection mechanisms are automatically applied and do not interfere with the work of the user.
7. Consistency
   Having consistent styles, colors, objects, wording, etc. Establish standard colors, have sequences of actions in a consistent order for similar situations and actions, use consistent and clear terminology throughout the system (avoid jargon), reuse, keep information short and to the point, use explicit words to classify risk levels, use consistent placement and controls, users should not have to wonder if different words, situations, or actions mean the same thing, use both knowledge in the world and knowledge in the head, and standardize when all else fails for stability and reliability.
8. Feedback
   Providing information to users about what can and has happened. Dialogues can be designed to yield closure where actions and information are grouped with a beginning, middle, and end with informative feedback at completion of each step, provide feedback when users have to wait as to what is going on and why, provide information and feedback as to why something happened (or didn't), and always have full and continuous information about results of actions and the current state of the system.
9. Errors and help
   Preventing errors as much as possible, and provide help. To the extent possible, design systems where users cannot make serious errors (and have well designed error messages), eliminate error-prone conditions, provide an easy option for users to enquire or complain, help users recognize, diagnose, and recover from errors, provide an easy way for users to

get help, technical support, and find documentation, provide fault tolerance by anticipating potential compromises and failures, improving redundancy and survivability of common and important tasks, and provide no external burden for users. Design for error (because it will happen).

10. Effectiveness and constraints

    Reducing user effort to support user and system performance, using constraints appropriately to reduce errors and increase effectiveness (physical, logical, semantic, and cultural restraints to guide actions), creating opportunity by taking advantage of object relationships and resources, drawing distinctions between objects and actions that are relevant to the task (what actions must be manipulated separately or together; what objects do users care/not care about), allowing the user to make decisions about what to show/hide, and the range of required tasks should be accomplished at a certain success level within a specific set amount of time by a specific percentage of users to be considered effective.

11. Efficiency

    Responsiveness and how the user perceives the rate of communication within a system (within an appropriate amount of time), how a system supports a user in their task(s), how quickly tasks can be performed once they have been learned, presenting few options to simplify choices and efficiency, following the principles of economy of mechanism by designing security measures that are as simple as possible with simple and straightforward structures (making it easier to test, update, and protect), and the system is designed for human efficiency before computer efficiency. To increase efficiency, include defaults by focusing on appropriate defaults for users regarding pre-selected or predetermined options and fail-safe defaults where access decisions are based on permission rather than exclusion.

12. Learnability

    How easy it is for users to accomplish tasks for the first time in a non-threatening system, support user mental models (synthesizability), tasks are generalizable to support the user and extend their knowledge of actions supported within the system and across other situations, and the system should display clues in a way that supports users in creating mental models.

13. Defense in depth

    Layering security to provide prevention, detection, and response, layering a system with overlapping protections that address people, technology, and operations, protecting the user from potentially dangerous conditions or undesirable situations, examining the consequences of loss and the likelihood of loss before and without implementation, examining risk management to find ways that risks can be mitigated, insurance acquired, or if the risk can be accepted and managed, tailoring security strategies to the magnitude of risks within practical constraints imposed by the system and environment, keeping security in balance with the needs and business benefits, and understand the possible vulnerabilities, exploits, and potential attackers.

14. Authority and privilege
    Maintaining accurate awareness of all authorities relevant to user decisions (the user's authority, device's authority, etc), informing the user of what authorities they are granting to different components, users, or applications and what those authorities mean and potential consequences, provide users a way to review and revoke the authorities that have been granted, providing complete mediation where every access to every object is checked for authority (not necessarily relying on a cache), verifying that other parties do not gain access that exceeds user expectations, protect the user's channels that allow them to manipulate authority and the agents that manipulate authority on the user's behalf (provide a trusted path), use the least amount of privilege necessary to complete a task, separate privileges for restricted resources to mitigate potential unauthorized access, and always require explicit authorization.
15. Privacy
    Explicitly stating the purpose of actions and data collection, providing standardized security policies that are easy to understand, can be audited, are clearly documented and accessible, and can be taught to users, providing a strong privacy environment throughout the system and help access and documentation, protecting data in accordance with the provisions of protection and accountability (especially with regards to biometric or personal data), keeping all personal and identifiable information on the user's personal computing environment and not transmit it outside of the environment (unless absolutely required, such as by law), limit the extent of personal data retained and exchanged to what is absolutely necessary and only for necessary operations and actions, maintain privacy logs so that users can have access to their own data and can correct it if necessary, providing information on when/how/if/ and with whom data could potentially be shared with and allowing users to consent or not to this, protect data from unauthorized access or disclosure, provide mechanisms for the protection of all steps performed by the system, and remember that there is no such thing as absolute security and privacy, but do what is necessary and possible to protect users' privacy and information.
16. Mappings
    The user's mental model and creating a system that helps the mental model by providing the path of least resistance (often the natural way to do a task should also be the secure way), providing an organized interface based on clear and consistent models that are recognizable to users, matching the most comfortable way to do tasks with the least granting of authority (greater risk should equal greater effort), not defaulting to restricting access, using icons and visual indicators to support mappings and mental models, creating predictability so that results are in accordance with previous commands and mappings, reducing short-term memory load, the interface design should match the user's mental model and should project all the required information to create a good conceptual model of the system (which leads to a feeling of user control), increase memorability so that when a

user returns to the system after a period of time, their mappings and mental models can easily be reestablished, match the mappings of the system to the real world and create familiarity, and use recognition rather than recall to reduce memory load, relearning time, and to increase the speed at which users can relearn the mappings of the system.

17. Security and authentication
    Providing functionality and assurance to a system by describing what a system should do, providing assurance requirements that describe how the functional requirements should be or have been implemented and tested, providing verification and validation, ensuring confidentiality, integrity, and availability of data and system, protecting system data from accidental changes or access, keeping data and resources available for authorized use, especially during potential emergencies (such as Denial of Service, loss of information capabilities, and equipment failures), provide warnings of potential surveillance or data access or use, enable users to express safe security policies in terms that fit their tasks, provide preventative, detective, and responsive security controls, provide open disclosure whenever possible, allow users to easily manage their authenticators, provide identity verification as long and as frequently as access to a resource or data is permitted, authentication should feel trivial to the genuine user, provide measures of confidence to humans for authentication, and good security now without waiting for something better or perfect.
18. Flexibility, customizability, and accessibility
    Making a system open and easy for a variety of users by allowing users to modify the interface of a system, design for plasticity and provide shortcuts, support multi-threading by allowing the system to support user interaction pertaining to several tasks at a time, ensure non-discrimination, allow users to tailor frequent actions, allow the interface and system to adapt to various environments and users, use explanatory tool tips for unfamiliar terms and processes, reduce complexity for increased accessibility, flexibility, and security, specify and enforce expected behaviors, actions, and processes (do not make assumptions), making sure that all functions and actions provide utility, and follow the principle of least common mechanism by reducing unintended communication paths and minimizing the number of shared functions.
19. Isolation
    System and data protection by reducing access from public systems (especially to critical resources), processes and files specific to the user being isolated from others, isolating security mechanisms to prevent unauthorized access to those mechanisms, encapsulating a collection of procedures and data so that internal structure of data is accessible at designated entry points, define and control how different aspects interact with each other by breaking apart, limiting, and controlling the underlying structure of systems, provide modularity in the development of security functions as separate and protected modules, and design to provide common security functions and services as common modules.

4.4 Evaluations

A total of six mobile phones and their corresponding biometric authentication methods were evaluated using the evaluation form created based on the guidelines (see Appendix A.6). Some guidelines were not evaluable due to a lack of information available to the general public or provided in the mobile phone interfaces. The purpose of the guidelines is more focused for during design and development, however they can also be used as an evaluation tool during and after implementation. The evaluations focused on the negative aspects of each device and what could be improved, and do not discuss the positive aspects of each device. Each phone evaluated is listed in Table 8.

Label for Evaluation	Phone Brand and Model	Authentication
Phone 1 (P1)	Apple iPhone XS Max - 2018	Face recognition
Phone 2 (P2)	Samsung Galaxy S9+ - 2018	Fingerprint, iris, and face recognition
Phone 3 (P3)	Blackberry Key2 - 2018	Fingerprint and face recognition
Phone 4 (P4)	Motorola Moto Z^3 Play - 2018	Fingerprint and face recognition
Phone 5 (P5)	Apple iPhone 7 - 2016	Fingerprint recognition
Phone 6 (P6)	Samsung Galaxy S8 - 2017	Fingerprint, iris, and face recognition

Table 8: Mobile phones used in the evaluations

The guidelines "Defense in Depth" and "Isolation" could not be determined during the evaluation of each mobile phone as they have more to do with the development of a system. The other 17 guidelines were evaluable, and each guideline was given a severity rating of Low, Medium, High, or Critical on the importance and criticality of each problem. Each evaluation took about 40-60 minutes to complete. An overview of the guidelines, each mobile phone, and their severity rating can be seen in Table 9. Black is used to show which guidelines could not be assessed during the evaluations, red is used for the severity rating critical, orange for high, yellow for medium, and almond for low.

Guideline	P1	P2	P3	P4	P5	P6
Visibility and discoverability	🟫	⬜	⬜	⬜	⬜	🟫
Clarity	🟨	🟨	🟧	⬜	⬜	🟨
Trust	⬜	🟨	🟨	⬜	🟨	🟨
User control and consent	🟨	🟨	🟨	🟨	🟨	🟫
Open and minimalist design	🟫	⬜	⬜	⬜	⬜	⬜
Psychological acceptability	⬜	⬜	⬜	⬜	🟨	⬜
Consistency	⬜	⬜	🟨	🟫	🟫	🟫
Feedback	🟨	🟫	🟥	🟨	🟨	⬜
Errors and help	🟨	🟨	🟨	🟨	🟨	🟨
Effectiveness and constraints	🟫	🟨	🟫	🟫	⬜	⬜
Efficiency	🟫	🟫	⬜	🟫	🟫	⬜
Learnability	🟨	🟨	🟨	🟫	🟨	🟨
Defense in depth	⬛	⬛	⬛	⬛	⬛	⬛
Authority and privilege	🟨	🟫	🟨	🟨	🟨	🟨
Privacy	🟫	🟨	🟨	🟨	🟫	🟨
Mappings	🟫	🟫	🟨	⬜	⬜	🟫
Security and authentication	🟫	🟧	🟥	🟫	🟨	🟨
Flexibility, customizability, and accessibility	🟨	🟫	🟨	⬜	🟨	🟨
Isolation	⬛	⬛	⬛	⬛	⬛	⬛

Table 9: Overview of each mobile phones' evaluation results with regards to severity rating

Two mobile phones, P1 and P6, were given a severity rating of Low for the guideline "Visibility and discoverability". P1 and P6 were both given this rating due to it not being apparent which biometric authentication method(s) were enabled on the lock screen except for fingerprint recognition on P6. The lock screen is virtually the same for whatever method is enabled. For the guideline "Clarity", P1, P2, and P6 were given the severity rating of Medium, and P3 was given a rating of High. Regarding P1, not all security actions and their results was apparent, so that if face recognition is used, the result is not apparent and must be recalled rather than recognized. The security preferences set up for P2 was not initially clear nor intuitive, and when iris or face recognition stop working while attempting to authenticate, it is not clear as to why. There is also no clear information on deleting data on P2 if the device is attacked by an imposter, such as if attacked incorrectly multiple times, the device data will be deleted. Regarding P6, there is a setting called "Preferred biometrics", and what that relates to is not initially clear, and is something that must be recalled. P3 was given a severity rating of High due to issues with enrollment for fingerprint authentication (the inability to do so), and there being no reason provided as to why.

Four mobile phones, P2, P3, P5, and P6, had a severity rating of Medium for the guideline "Trust". These devices provided little to no disclosure on biometric data collected, its usage, or how it could be used, leading to the severity rating of Medium. The guideline "User control and consent" was an issue with every mobile phone. P1-P5 were given a severity rating of Medium, whereas P6 was given a severity rating of Low. Regarding P1, there was not always feedback provided on what a user action would result in nor was there always verification for informed consent, so a user could accidentally hit a button and the action would be completed without asking the user if they were sure. P2, P3, and P4 did not provide explicit consent all the time, and there was no recoverability of deleted data. P6 was provided a rating of Low due to the lack of reversibility of deleted data, but it had informed consent beforehand unlike the other devices.

P1 was the only device given a severity rating for "Open and minimalist design", with a rating of Low. This was due to a difference between sections of information in the biometrics and security settings not being clear. "Psychological acceptability" had a severity rating of Medium with P5. This was because of a lack of verification, consent, and revocability. P4, P5, and P6 were given a severity rating of Low for the guideline "Consistency", and P3 was given a rating of Medium for the same guideline. With regards to P4, access to fingerprint and face recognition data were not consistent with each other, and fingerprint recognition could be set up without another authentication method enabled, but this was not the case for face recognition. The set up phases for fingerprint recognition were not consistent for P5, and P6 requires a user to swipe the screen first to use iris recognition, however that is not the case for face or fingerprint recognition. P3 was given a rating of Medium due to fingerprint and face recognition not being located in similar areas of the settings, and face recognition being in a way hidden.

"Feedback" had severity ratings of Low (P2), Medium (P1, P4, and P5), and Critical (P3). P2 had reduced feedback when face or iris recognition was used to authenticate a user, with reduced feedback that iris was accepted. Regarding the severity rating of Medium, P1 provided no tactile feedback during enrollment or verification, nor was there feedback before deleting biometric data. P4 and P5 also did not have feedback or verification for the deletion of data. P3 was given a severity rating of Critical due to the inability to enroll in fingerprint recognition with no feedback as to why or what was happening. Every mobile phone had a severity rating of Medium for "Errors and help". None of the devices provided a help function for biometric authentication or regarding biometric data. P1 also had an issue with face recognition data, where multiple faces could be enrolled, but individual ones could not be deleted. Either everything was kept or everything was deleted. P3 also provided no help with enrollment, which was especially an issue due to the inability to enroll in fingerprint recognition on that device.

Three mobile phones (P1, P3, and P4) were given a severity rating of Low for "Effectiveness and constraints", and one mobile phone (P2) was given a rating of Medium. A user must swipe from the bar at the bottom of the screen to finish the unlocking process for P1, and P3 and P4 also had to swipe to finish unlocking the screen. The screen needed to be turned on for P2 to use iris recognition, the defaults for face recognition were faster but less secure, and it is not clear where to pick the primary authentication method initially, which led to the severity rating of Medium. Mobile phones P1, P2, P4, and P5 were given a severity rating of Low for the guideline "Efficiency". Swipe is required for P1 to complete the unlocking process and the device must be moved away from the face to be detected. P2 also requires swiping, but it is not default for intelligence scan, and face recognition does not work with sunglasses. P4 could use face recognition to unlock the screen, but if the screen was not turned on first it had to be swiped afterwards, and P5 required the fingerprint sensor to be pressed to be read.

The guideline "Learnability" had issues on every mobile phone, with P1, P2, P3, P5, and P6 given a severity rating of Medium, and P4 was given a rating of Low. P4 provided minimal information and introduction to face and fingerprint recognition. P1, P2, P3, P5, and P6 had no introduction to biometric authentication. P5 had a slight introduction to iris recognition, P3 had severe inconsistencies in the set up and placement of biometric authentication, and P2's biometric preferences set up is not initially clear. Mobile phones P1, P3, P4, P5, and P6 were given a severity rating of Medium and P2 was given a rating of Low for the guideline "Authority and privilege". P2 provided two different locations for the deletion of biometric data, which could cause confusion, leading to a rating of Low. P1 was not clear if revoking privilege for an app also removes biometric data associated with the app, and the amount of privilege granted was not clear, resulting in a rating of Medium. With P3, P4, P5, and P6, a user cannot tell what privileges and authorities are granted to where or how much, leading to a severity rating of Medium.

For the guideline "Privacy", P1 and P5 had a severity rating of Low, and P2, P3, P4, and P6 had a rating of Medium. P1 users cannot partially consent to anything, and P5 is only clear about some locations in which biometric data can be used, but no information about storing, collecting, or using data. P2, P4, and P6 do not provide explicit statements of data usage, purpose, or how it is stored and collected, resulting in a severity rating of Medium. P1, P2, and P6 had a severity rating of Low for "Mappings" and P3 had a rating of Medium for the same guideline. P1 provides several steps that must be followed to find information on data and privacy that does not match user mental models, and P2 and P6 have mappings that are not very intuitive and may not match user mental models, all leading to a rating of Low. And the device P3 did not have consistent mappings leading to increased recall rather than recognition.

Every mobile phone had issues for the guideline "Security and authentication", with P1 and P4 given a severity rating of Low, P5 and P6 given a rating of Medium, P2 a rating of High, and P3 a rating of Critical. P1 and P4 provided no information on how the data may be used or stored. Also, P2 provided a non-specific warning that fingerprint authentication can be used for apps and purchases, leading to a severity rating of Low but potentially Medium. P5 only provided minimal data on a few locations in which biometric data can be used, P6 defaults to less security so that face recognition is "faster", and neither P5 nor P6 provide information on data collection, storage, or usage. P2 had no verification for fingerprint set up, no information on storage, use, or collection, and no warnings that it could be used somewhere else, leading to a rating of High. And P3 was given a rating of Critical due to the issues with set up of fingerprint recognition and minimal data being provided for face recognition.

For the final guideline that was evaluated, P2 was given a severity rating of Low for "Flexibility, customizability, and accessibility", and P1, P3, P5, and P6 were given ratings of Medium. There was no tactile or audible feedback for verification of fingerprint recognition, and only one face or iris can be used, leading to a rating of Low. Only one option was available on P1 and P5, reducing its flexibility and accessibility, leading to a rating of Medium. P3 was given a rating of Medium due to difficulties in the set up for fingerprint recognition, although face recognition worked. And finally, P6 requires users to go into separate settings from the primary set up for authentication for a rating of Medium.

5 Discussion

Through Chapter 2, a clear answer to the first research question is found; there is indeed a relationship between usability and biometric authentication. The two sub-questions to the first question were "Is there a trade-off between usability and security" and "How have usability and biometric authentication been evaluated in mobile phones?". As to the first sub-question, the research, survey, and interviews seem to show overall that there is a trade-off. However there seems to be a shift happening in this line of thinking of a trade-off not necessarily being a negative thing, or that when "done right", there is a reduced trade-off or potentially no trade-off between usability and security. For the second sub-question, sections 2.3 and 2.4 explored several evaluation methods that have been used for evaluating usability and biometric authentication in mobile phones. Another potential evaluation method has been developed through this thesis based on the evaluation methods in sections 2.3, 2.4, further research that was conducted, and the testing discussed in Chapter 3 and 4.

5.1 Survey and interviews

Overall, the results obtained through the survey conducted show corroboration with the results found in Zirjawi et al. (2015), Lovisotto et al. (2017), and Al Abdulwahid et al. (2015) (Allen & Komandur 2019). This is specifically true in regards to there being a belief of security being an important aspect of mobile phone usage outside of the security profession. 76% of participants chose biometrics as the most secure authentication method, with pins and passwords as the second most common choice at 22%, which is akin to what Zirjawi et al. (2015) found. Pins and passwords are a commonly used authentication method, however the data collected appears to show their usage decreasing and the usage of biometric authentication to be increasing.

During the data analysis of the survey data, it was noted that the perceptions and understanding of usability was different than expected. Outside of those who work in the usability or related fields, the number of participants who said that they have an advanced or expert understanding of usability was fairly high, which could be in part due to the simplified definition provided in the survey. In regards to both usability and biometrics, there was a fairly similar percentage of participants who had an intermediate or novice understanding (39% for usability and 42% for biometrics). However, when looking at the advanced or expert understanding of usability and biometrics, the scores appear to correlate somewhat with the number of participants in each of the user groups, and there was a higher percentage of biometrics and security experts and general population participants who said that they had an advanced or expert understanding of usability than there were of usability participants who said that they had an advanced or expert understanding of biometrics.

Similar to Lovisotto et al. (2017), Zirjawi et al. (2015), fingerprint authentication was shown to be the biometric trait that was most preferred and used by mobile phone users. However, this is likely due to the fact that a majority of mobile phones with biometric authentication methods have had fingerprint authentication for several years, whereas biometric authentication methods like face recognition and iris recognition are more recently being used as common authentication methods on mobile phones in the past couple of years.

There was some similarity in the survey results about convenience and security compared to Lovisotto et al. (2017). Lovisotto et al. (2017) found that participants believed biometrics to be more secure (83%) and convenient (92%) than passwords, however those percentages were a bit lower in the survey that was conducted here at about 76% and 78% respectively. This survey also showed a lower percentage of participants who have used or currently use biometric authentication at 79% of participants, whereas Lovisotto et al. (2017) has results showing that 92% of their participants have used biometrics. This could be in part due to the differences in the participant samples, and could also be due to the number of participants and how those participants were found.

The survey also showed how both security and ease of use are important to users, where participants on average provided a score of 5 on a scale of 1-5 for the importance of both. This shows how there has been a shift in the thinking of mobile phone users, and how it is not just about one or the other; mobile phone users have a desire to use devices that do not have much of a trade-off (if any at all) between usability and security. Participants have also shown that convenience is also important, and that even if an authentication method is secure, if it is not easy to use or convenient, many participants won't use that method.

There were several common details that arose throughout the interviews. Several participants talked about how "usability is a large reason as to why biometric authentication is used", and how today there is variation in the usability level of different biometric authentication methods on different phones (Allen & Komandur 2019). Several participants also discussed how "humans are an important factor that are often overlooked or thought of as a problem when it comes to authentication". There was also discussion on how users circumvent security if it is not usable, which is not a good situation to be in. Usability and security should not clash or get in the way of each other, but support each other. Many of the participants said that there is a trade-off between usability and security, yet this is not necessarily a bad thing or problem. Perhaps by this they are trying to say that a balance can be attained where there is a good level of both usability and security.

The data from the interviews supports the data from the surveys. Interview participants discussed how users are dependent on things that are easy to use and like things that are convenient for them. They also discussed similar concerns about FAR and FRR, and that in practice, mobile phones are not always both secure and usable. Both participant samples believed that there is a trade-off between usability and security, however in the interviews several participants discussed how this is not necessarily a bad thing or something that cannot change.

After conducting the survey and interviews, the second and third research questions could be examined. These questions were: "Are the perceptions from those working in the usability field and biometrics/computer security field in line with each other?" and "Are the perceptions of those working in the usability field and biometrics/computer security field in line with that of the literature?". Concerning the first of these two research questions, it can be shown that security and biometrics experts have more experience using biometric authentication methods, however when it came to which authentication methods that both participant groups thought was most secure, convenient, and easy to use, they provided similar scores (83-91% from biometrics and security experts and 73-90% from usability experts). When participants were asked if they use biometric authentication, why, both user groups had a majority of participants mention ease of use and convenience, with some participants in both user groups mentioning the security of biometric authentication. Participants from both user groups also mentioned similar concerns and views of current biometric authentication. From the interviews, there were common themes where participants from both user groups mentioned how users like consistency and things that are easy to use. These participants also discussed similar concerns that emerged from the survey. Altogether, based on the information collected from the survey and interviews, it can be said that yes, the perceptions of those working in the biometrics and security field and those working in the usability or related fields are similar, and overall in line with each other.

With regards to the second of these two questions, both the literature and survey show that there is a common belief that security and usability are linked. 76% of survey participants said that there is a link between the two, and the interview participants also showed that they believed there to be a link. The literature shows a link between usability and security, however there are still some mixed results on whether that link can be a negative or positive thing. When it comes to a trade-off, 52% of participants in the survey said that there is a trade-off between usability and security as well as a majority of the interview participants. A couple of survey participants also discuss how there is a trade-off now, but that it may change in the future. Furthermore, most of the interview participants stated that there is a trade-off as well. In the literature, there are several sources that state that there is a trade-off between security and usability, but many of the sources talk about finding the balance between the two or that the trade-off can be reduced or removed with effort. This was also discussed in some of the interviews. From the data collected, it could also be shown that with an increased understanding of usability or biometrics, there was an increase in the likelihood that a participant would believe that there is a link between the two. From the data collected and discussed in Chapters 2 and 4, it can be inferred that the perceptions of those working in the usability, biometrics, security, and related fields is in line with that of the literature.

5.2 Guidelines

As has been previously discussed, the purpose of the guidelines created during this thesis was to develop a set of guidelines that could be used as a guide for the design and development or evaluation of biometric authentication in mobile phones for increased usability and security, or usable security. There are several individual guidelines that have a focus on either usability (such as open and minimalist design) or security (such as defense in depth), and there are also several individual guidelines that address both security and usability concerns (such as errors and help). However, most guidelines, like the ones shown in Tables 2-5 predominantly focus on either usability or security. Considering that there has often been a perceived trade-off between the two, it can be difficult to design and develop systems that are both secure and usable, as most guidelines and teams tend to focus on one or the other.

There have not been many guidelines created that focus on both security and usability, which is why the guidelines created here can be considered to be a more comprehensive approach than the other guidelines that have been created that predominantly focus on either security or usability. Out of all of the guideline sets used in the development of these guidelines, only Yee (2002), Johnston et al. (2003), Yee (2005), and Garfinkel (2005) discuss both usability and security. Nevertheless, these guidelines do not take into account authentication specifically. The guidelines developed here can thus be considered to be potentially more comprehensive than the four guidelines mentioned, however they must be further tested and evaluated. These guidelines have also been designed with mobile phones specifically in mind, which means that they may not be as applicable to other technological use cases. To be able to use the guidelines as a guide and/or evaluation tool, it is especially helpful if there are team members who understand either security or usability (or both), so that each guideline can be followed and evaluated to as much of an extent as possible for the best feasible results, which can occasionally prove to be difficult in some teams or companies that focus on one or the other.

As previously mentioned, these guidelines were developed with a particular use case in mind, that being biometric authentication in mobile phones. This was done to satisfy a growing use case, however as a result this means that these guidelines should not be used in non-mobile phone related use cases, which can be limiting. They could potentially be applicable to tablets, however as they currently stand there is only one use case in which they are recommended to be used. As an evaluation tool, the guidelines were created to be able to assess security, usability, and authentication aspects in this use case, whereas usually for this to be done, several evaluation methods would need to be used. And as a guide for design and development, these guidelines can be used as a tool to reference and direct the design and development mobile phone authentication that is both secure and usable, where previously there has not been a comprehensive list such as this to use in similar use cases.

5.3 Evaluations

The severity scores provided were based on the researchers personal opinions and were attempted to be as consistent as possible. However, as the evaluations were conducted by a single person, all ratings should be taken with a grain of salt and future evaluations should be conducted by several people with varying expertise levels in usability, security, biometrics, authentication, or none of the above. Also, it should be clarified that the mobile phones used in these evaluations are devices that are actively in use by mobile phone users, not brand-new phones straight out of the box or on display at stores, so some of the results could change if the phones were in a store or fresh from a box.

Some of the devices evaluated had something that was unique in a way that could benefit users according to the guidelines. P1 was fairly clear about the usage of the biometric data collected and what other apps had access to that data (or could have access). P2 provided tips for the use of iris recognition, which could be especially useful as iris recognition is still relatively new as a biometric authentication method in mobile phones. P3 had an option to "Improve face-matching" where users could scan their face multiple times in different settings. P3 also may have had issues with fingerprint enrollment due to previous issues with that specific phones' space bar (where the sensor is placed for fingerprint authentication).

The evaluations conducted here do not take into account presentation attack detection or imposters attempting to access the devices. That is something that must be tested for as well that is outside of the scope of the guidelines created here. However, presentation attack detection should be considered when developing and designing systems relating to guidelines #3 (Trust), #4 (Use control and consent), #5 (Open and minimalist design), #13 (Defense in depth), #15 (Privacy) #17 (Security and authentication), and #19 (Isolation).

Based on all of this, research question number four can be discussed. The research question was "Can usability and biometric authentication be more effectively incorporated in the beginning of the design and development process?". This question is one that cannot be easily answered, as it is something that most likely must be looked at over the span of several years. However, the evaluations conducted here show different paths that mobile phone developers have taken on the way to increased usability and biometric authentication. The hope is that the guidelines created and evaluated here could be used to increase both security and usability in biometric authentication in mobile phones, as the guidelines take into account several important factors that usually require several sets of guidelines. Also, based on the survey conducted in Chapter 4 and the surveys and evaluations reviewed in 2, it is apparent that there has been increased usage of biometric authentication, and overall an increase in acceptance and satisfaction in using biometric authentication in mobile phones, which is likely due to the improved usability thus far. However, as has been discussed, both usability and security can further be increased in mobile phones, and the guidelines created here aim to do just that. Based on the results of the guidelines, it appears that they can indeed be used to find areas in both security and usability that can be improved as either an evaluation form or as a guide during design and development.

5.4 Limitations

As with every study, there are limitations. One of the larger limitations of this study was the time-constraint. Only so much can be accomplished in a master's thesis, and this has an effect on the results. During the survey and interview data collection, the participant sample was primarily a convenience sample and under 100 total participants, meaning that the data collected is not fully generalizable to the wider population nor fully representative of the three user groups (usability experts, security/biometrics experts, and the general population). One of the user groups also had under 30 participants in the survey, thus reducing its generalizability. When conducting a survey, it is not possible to validate that the participants understood the questions properly nor is it possible to ask participants to elaborate, so this is also a limitation. There is also chance for survey and interview bias where participants answer in a manner that they think is "desirable" or they cannot accurately express their beliefs (Baxter et al. 2015). Both the survey and interviews were conducted in English, however not all participants were native English speakers, which could introduce some confusion when reading the questions and responding.

In regards to the guidelines that were developed and evaluated, the guidelines need further and more in-depth testing. The evaluations were also conducted by the researcher who created them, so it is not clear what would happen if another were to conduct the evaluations and how understandable the evaluation form and guidelines would be. Another limitation concerning the evaluations is that the researcher has primarily used mobile phones from one particular brand, so that can introduce some bias in the evaluation results.

6 Conclusion

Usability and security are both growing concerns in today's society, and biometric authentication in mobile phones must be both secure and usable with societies increasing reliance on them. With the ever increasing importance of security, biometric authentication is a strong option that with some work, can be practically more secure and usable than traditional authentication methods like passwords, pins, and patterns, not just theoretically more secure and usable. It is apparent that all user groups surveyed and interviewed see that there is indeed a link between usability and security (Allen & Komandur 2019), and the literature in 2 furthermore supports this. The debate as to whether one increases while the other decreases has declined, however we as a society need to make sure that there is a strong emphasis on both usability and security, not one or the other. This thesis has explored the relationship between security and usability in regards to biometric authentication in mobile phones. However, there is still more work to be done, and the guidelines that have been established are a way to further explore the usability of biometric authentication in mobile phones.

6.1 Future Work

Future work in regards to this topic should focus on the guidelines that have been established. The guidelines should be reviewed and be put through a few iterations based on the evaluations conducted and further research. The guidelines should also be tested in the design and development of biometric authentication in a mobile phone to evaluate their usefulness and possibility of increasing usability and security to attempt to more completely answer research question four. These guidelines could also be a way to bring usability and security experts together so that neither usability nor security will be added on as a "feature", but are fully implemented for the best results possible.

Bibliography

Ackerman, M. & Mainwaring, S. (2005), Privacy issues and human-computer interaction, *in* 'Security and Usability: Designing secure systems that people can use', O'Reilly, chapter 19, pp. 381–399.

Adams, A. & Sasse, A. (2005), Users are not the enemy, *in* 'Security and Usability: Designing secure systems that people can use', O'Reilly, chapter 32, pp. 639–649.

Ahmed, I. U. (2017), *Smartphone Authentication: User experience, expectation and satisfaction*, Master's thesis, Lappeenranta University of Technology. Retrieved from: `http://lutpub.lut.fi/bitstream/handle/10024/143330/mastersthesis_ahmed_imtiaz.pdf?sequence=2`.

Al Abdulwahid, A., Clarke, N., Stengel, I., Furnell, S. & Reich, C. (2015), Security, privacy and usability – a survey of users' perceptions and attitudes, *in* '*Trust, Privacy and Security in Digital Business*', Springer International Publishing, pp. 153–168. doi:10.1007/978-3-319-22906-5_12.

Allen, C. & Komandur, S. (2019), The relationship between usability and biometric authentication in mobile phones, *in* '*Communications in Computer and Information Science*', Springer International Publishing. Forthcoming.

Alshamari, M. (2016), 'A review of gaps between usability and security/privacy', *International Journal of Communications, Network and System Sciences* **09**, 413–429. doi: 10.4236/ijcns.2016.910034.

Ashbourn, J. (2000), *Biometrics: Advanced Identity Verification*, Springer Link.

Attaullah, B., Akhtar, Z., Crispo, B. & Gupta, S. (2017), Mobile biometrics: Towards a comprehensive evaluation methodology, *in* '*51st International Carnahan Conference on Security Technology (ICCST-17)*'. doi: 10.1109/CCST.2017.8167859.

Authentication (n.d.), In *Merriam-Webster Online*. Retrieved from: `https://www.merriam-webster.com/dictionary/authentication`.

Baxter, K., Courage, C. & Caine, K. (2015), *Understanding your users: A practical guide to user research methods*, 2nd edn, Morgan Kaufmann, Amsterdam, Netherlands.

Ben-Asher, N., Meyer, J., Möller, S. & Englert, R. (2009), An experimental system for studying the tradeoff between usability and security, *in* '*2009 International Conference on Availability, Reliability and Security*', pp. 882–887. doi: 10.1109/ARES.2009.174.

Bhagavatula, C., Ur, B., Iacovino, K., Mon Kywe, S., Cranor, L. & Savvides, M. (2015), Biometric authentication on iphone and android: Usability, perceptions, and influences on adoption, *in* '*Workshop on Usable Security at USEC '15*'. doi: 10.14722/usec.2015.23003.

Biometrics Institute (2017), 'Biometrics privacy guidelines: A best practice guide for biometrics and privacy'. Retrieved from: `https://www.biometricsinstitute.org/wp-content/uploads/BiometricsInstitutePrivacyGuidelines2017.pdf`.

Bishop, M. (2005), Psychological acceptability revisited, *in* 'Security and Usability: Designing secure systems that people can use', O'Reilly, chapter 1, pp. 1–11.

Blanco-Gonzalo, R., Diaz-Fernandez, L., Miguel-Hurtado, O. & Sanchez-Reillo, R. (2013), Usability evaluation of biometrics in mobile environments, *in* '*2013 6th International Conference on Human System Interactions (HSI)*'. doi: 10.1109/hsi.2013.6577812.

Braz, C., Seffah, A. & M'Raihi, D. (2007), Designing a trade-off between usability and security: A metrics based-model, *in* '*Lecture Notes in Computer Science Human-Computer Interaction – INTERACT 2007*', pp. 114–126. doi: 10.1007/978-3-540-74800-7_9.

Braz, C., Seffah, A. & Naqvi, B. (2018), *Integrating a Usable Security Protocol into User Authentication Services Design Process*, CRC Press - Taylor & Francis Group, LLC.

Brostoff, G. (2017), 'Adoption problems? how ux could boost biometrics', *Biometric Technology Today* **2017**(9), 9–11. doi: 10.1016/S0969-4765(17)30167-4.

Böhm, I. & Testor, F. (2004), 'Biometric systems', *Department of Telecooperation University of Linz, 4040* . Retrieved from: `https://myocoms.com.ng/ebooks/biometrics04.pdf`.

Computer security (2019), In *Encyclopædia Britannica, Inc.* Retrieved from: `https://www.britannica.com/technology/computer-security`.

Coventry, L. (2005), Usable biometrics, *in* 'Security and Usability: Designing secure systems that people can use', O'Reilly, chapter 10, pp. 181–203. Retrieved from: `https://pdfs.semanticscholar.org/9b8b/227d8fc36eddaf3fa5d8828c1eeb8255c3ce.pdf`.

Cranor, L. F. & Buchler, N. (2014), 'Better together: Usability and security go hand in hand', *IEEE Security Privacy* **12**(6), 89–93. doi: 10.1109/MSP.2014.109.

Cranor, L. & Garfinkel, S. (2004), 'Guest editors' introduction: Secure or usable?', *Security & Privacy, IEEE* **2**, 16 – 18. doi: 10.1109/MSP.2004.69.

Cranor, L. & Garfinkel, S. (2005), *Security and Usability: Designing secure systems that people can use*, O'Reilly.

Dix, A. (2004), *Human-Computer Interaction*, 3 edn, Pearson Prentice-Hall.

El-Abed, M., Giot, R., Hemery, B. & Rosenberger, C. (2010), A study of users' acceptance and satisfaction of biometric systems, *in* '44th Annual 2010 IEEE International Carnahan Conference on Security Technology', pp. 170–178. doi: 10.1109/CCST.2010.5678678.

FIDO Alliance (2014), 'Fido: Fast identity online alliance privacy principles'. Retrieved from: `https://fidoalliance.org/wp-content/uploads/2014/12/FIDO_Alliance_Whitepaper_Privacy_Principles.pdf`.

Find Biometrics (2016), 'All smartphones shipped in 2018 will feature biometric tech: Acuity'. Retrieved from: `https://findbiometrics.com/smartphones-biometric-tech-acuity-307221/`.

Friedman, B., Lin, P. & Miller, J. (2005), Informed consent by design, *in* 'Security and Usability: Designing secure systems that people can use', O'Reilly, chapter 24, pp. 495–521.

Garfinkel, S. (2005), Design principles and patterns for computer systems that are simultaneously secure and usable, PhD thesis, Massachusetts Institute of Technology, Dept. of Electrical Engineering and Computer Science. Retrieved from: `https://simson.net/thesis/thesis.pdf`.

Gonzalo, R. (2016), Usability in Biometric Recognition Systems, PhD thesis, Universidad Carlos III de Madrid. Retrieved from: `https://e-archivo.uc3m.es/bitstream/handle/10016/23210/tesis_ramon_blanco_gonzalo_2016.pdf`.

Gray, D., Brown, S. & James, M. (2010), *Gamestorming: A Playbook for Innovators, Rulebreakers, and Changemakers*, O'Reilly Media, Inc.

Griffin, A. (2016), 'iphones are unlocked 80 times per day, apple says as part of security briefing', *The Independent UK* . Retrieved from: `https://www.independent.co.uk/life-style/gadgets-and-tech/news/iphone-unlock-apple-phone-security-privacy-touch-id-fingerprint-sensor-a6990701.html`.

Hess, W. (2010), 'Guiding principles for ux designers'. Retrieved from: `https://uxmag.com/articles/guiding-principles-for-ux-designers`.

Ibrahim, T., Furnell, S. M., Papadaki, M. & Clarke, N. L. (2010), Assessing the usability of end-user security software, *in* 'Trust, Privacy and Security in Digital Business', Springer Berlin Heidelberg, pp. 177–189.

Interaction Design Foundation (n.d.), '*What is Usability?*'. Retrieved from: `https://www.interaction-design.org/literature/topics/usability`.

Johnston, J., Eloff, J. & Labuschagne, L. (2003), 'Security and human computer interfaces', *Computers & Security* **22**(8), 675 – 684. doi: 10.1016/S0167-4048(03)00006-3.

Kainda, R., Fléchais, I. & Roscoe, A. (2010), Security and usability: Analysis and evaluation, *in* '2010 International Conference on Availability, Reliability and Security'. doi: 10.1109/ares.2010.77.

Labati, R. D., Piuri, V. & Scotti, F. (2012), Biometrics privacy protection: Guidelines and technologies, *in* 'E-Business and Telecommunications', Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 3–19. Retrieved from: `https://link.springer.com/chapter/10.1007/978-3-642-35755-8_1`.

Lederer, S., Hong, J., Dey, A. & Landay, J. (2005), Five pitfalls in the design for privacy, *in* 'Security and Usability: Designing secure systems that people can use', O'Reilly, chapter 21, pp. 421–446.

Lockwood, L. A. D. & Constantine, L. L. (2003), Usability by inspection : Collaborative techniques for software and web applications, *in* 'USE 2003 Performance by Design: Proceedings of the Second International Conference on Usage-Centered Design'. Retrieved from: `https://pdfs.semanticscholar.org/bcbf/86705b45953645602252ff772fbfa9b8a5db.pdf?_ga=2.245541511.2043567760.1553262356-1254879359.1551708740`.

Lovisotto, G., Malik, R., Sluganovic, I., Roeschlin, M., Trueman, P. & Martinovic, I. (2017), '*Mobile Biometrics in Financial Services: A Five Factor Framework*', Department of Computer Science, University of Oxford. Retrieved from: `https://newsroom.mastercard.com/eu/files/2017/06/Mobile-Biometrics-in-Financial-Services_A-Five-Factor-Framework-compressed3.pdf`.

Matyas, V. & Riha, Z. (2002), Biometric authentication - security and usability, *in* 'Advanced Communications and Multimedia Security: IFIP TC6 / TC11 Sixth Joint Working Conference on Communications and Multimedia Security', pp. 227–239. doi: 10.1007/978-0-387-35612-9_17.

Mayron, L., Hausawi, Y. & Bahr, G. (2013), Secure, usable biometric authentication systems, *in* 'UAHCI 2013: Universal Access in Human-Computer Interaction. Design Methods, Tools, and Interaction Techniques for eInclusion', pp. 195–204. doi: 10.1007/978-3-642-39188-0_21.

Merkow, M. S. & Breithaupt, J. (2014), *Information security: principles and practices*, Pearson. Retrieved from: `https://www.safaribooksonline.com/library/view/information-security-principles/9780133589412/?ar&orpq`.

Mihajlov, M., Blazic, B. J. & Josimovski, S. (2011), Quantifying usability and security in authentication, *in* '2011 IEEE 35th Annual Computer Software and Applications Conference', pp. 626–629. doi: 10.1109/COMPSAC.2011.87.

Mohamed, M. A., Chakraborty, J. & Dehlinger, J. (2017), 'Trading off usability and security in user interface design through mental models', *Behaviour & Information Technology* **36**(5), 493–516. doi: 10.1080/0144929X.2016.1262897.

Nielsen, J. (1994), '10 heuristics for user interface design', Nielsen Norman Group. Retrieved from: https://www.nngroup.com/articles/ten-usability-heuristics/.

Nielsen, J. (2000), '*Security and Human Factors*', Nielsen Norman Group. Retrieved from: https://www.nngroup.com/articles/security-and-human-factors/.

Nielsen, J. (2012), '*Usability 101: Introduction to Usability*', Nielsen Norman Group. Retrieved from: https://www.nngroup.com/articles/usability-101-introduction-to-usability/.

Norman, D. (2013), *The Design of Everyday Things*, Revised and Expanded edn, Basic Books.

Oluwatosin Nwokedi, U., Amunga, B. & Bashari Rad, B. (2016), 'Usability and security in user interface design: A systematic literature review', *International Journal of Information Technology and Computer Science* **8**, 72–80. doi: 10.5815/ijitcs.2016.05.08.

P. Kukula, E., Sutton, M. & Elliott, S. (2010), 'The human–biometric-sensor interaction evaluation method: Biometric performance and usability measurements', *Instrumentation and Measurement, IEEE Transactions on* **59**, 784 – 791. doi: 10.1109/TIM.2009.2037878.

Patrick, A. (2004), Usability and acceptability of biometric security systems, *in* '*International Conference on Financial Cryptography*', Vol. 3110, p. 105.

Patrick, A. (2008), *Fingerprint Concerns: Performance, Usability, and Acceptance of Fingerprint Biometric Systems*. Unpublished. Retrieved from: https://tinyurl.com/patrick-fingerprintconcerns.

Patrick, A., Briggs, P. & Marsh, S. (2005), Design systems that people will trust, *in* 'Security and Usability: Designing secure systems that people can use', O'Reilly, chapter 5, pp. 75–99.

Peisert, S., Talbot, E. & Kroeger, T. (2013), 'Principles of authentication'. Retrieved from: https://escholarship.org/uc/item/57b559jb.

Pocovnicu, A. (2009), 'Biometric security for cell phones', *Informatica Economica* **13**, 57–63. Retrieved from: https://search.proquest.com/docview/236781585?accountid=12870.

Preece, J., Rogers, Y. & Sharp, H. (2015), *Interaction design: beyond human-computer interaction*, 4 edn, John Wiley & Sons, Inc.

Renaud, K. (2005), Evaluating authentication mechanisms, *in* 'Security and Usability: Designing secure systems that people can use', O'Reilly, chapter 6, pp. 103–128.

Riley, C. W., Buckner, K., Johnson, G. & Benyon, D. (2008), 'Culture & biometrics: regional differences in the perception of biometric authentication technologies', *AI & society* **24**, 295–306. doi: 10.1007/s00146-009-0218-1.

Rogowski, M., Saeed, K., Rybnik, M., Tabedzki, M. & Adamski, M. (2013), 'User authentication for mobile devices', **8104**, 47–58. doi: 10.1007/978-3-642-40925-7_5.

Sahar, F. (2013), 'Tradeoffs between usability and security', *International Journal of Engineering and Technology* pp. 434–437. doi: 10.7763/IJET.2014.V5.591.

Saltzer, J. H. & Schroeder, M. P. (1975), 'Protection of information in computer systems', *IEEE CSIT Newsletter* **63**(9), 1280–1308. doi: 10.1109/CSIT.1975.6498831.

Sasse, A. (2004), '*Usability and trust in information systems*'. Retrieved from: http://discovery.ucl.ac.uk/20346/2/forsight.pdf.

Sasse, A., Brostoff, S. & Weirich, D. (2001), 'Transforming the 'weakest link' — a human/computer interaction approach to usable and effective security', *BT Technology Journal* **19**. doi: 10.1023/A:1011902718709.

Sasse, A. & Flechais, I. (2005), Usable security: Why do we need it? how do we get it?, *in* 'Security and Usability: Designing secure systems that people can use', O'Reilly, chapter 2, pp. 13–30.

Sasse, M. A., Smith, M., Herley, C., Lipford, H. & Vaniea, K. (2016), 'Debunking security-usability tradeoff myths', *IEEE Security Privacy* **14**(5), 33–39. doi: 10.1109/MSP.2016.110.

Schultz, E. E., Proctor, R. W., Lien, M.-C. & Salvendy, G. (2001), 'Usability and security an appraisal of usability issues in information security methods', *Computers & Security* **20**, 620–634. doi: 10.1016/S0167-4048(01)00712-X.

Shneiderman, B. & Plaisant, C. (2005), *Human-Computer Interaction*, 4 edn, Pearson Education, Inc.

Sollie, R. (2005), Security and usability assessment of several authentication technologies, Master's thesis, Gjøvik University College. Retrieved from: https://brage.bibsys.no/xmlui/handle/11250/143896.

Sons, S., Jackson, C. & Russell, S. (2017), *Security from First Principles*, O'Rielly. Retrieved from: https://www.safaribooksonline.com/library/view/security-from-first/9781491996911/?ar&orpq.

Stallings, W. & Brown, L. (2015), *Computer Security: Principles and Practice*, 3rd edn, Pearson Education Limited, England.

Tognazzini, B. (2005), Design for usability, *in* 'Security and Usability: Designing secure systems that people can use', O'Reilly, chapter 3, pp. 31–46.

Trade-off (n.d.), In *Merriam-Webster Online*. Def. 1 & 2. Retrieved from: https://www.merriam-webster.com/dictionary/trade-off.

Trewin, S., Swart, C., Koved, L., Martino, J., Singh, K. & Ben-David, S. (2012), Biometric authentication on a mobile device: A study of user effort, error and task disruption, *in* 'Proceedings of the 28th Annual Computer Security Applications Conference', ACM, pp. 159–168. doi: 10.1145/2420950.2420976.

Yee, K.-P. (2002), User interaction design for secure systems, *in* 'Information and Communications Security', Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 278–290. Retrieved from: `https://link.springer.com/chapter/10.1007/3-540-36159-6_24`.

Yee, K.-P. (2004), 'Aligning security and usability', *IEEE Security Privacy* **2**(5), 48–55. doi: 10.1109/MSP.2004.64.

Yee, K.-P. (2005), Guidelines and strategies for secure interaction design, *in* 'Usability and Security: Designing Secure Systems That People Can Use', O'Reilly, chapter 13, pp. 253–279. Retrieved from: `http://labs.toolness.com/temp/sid/ch13yee.pdf`.

Yong Gu, J., Jun Ho, P., Cheol, L. & Myung Hwan, Y. (2006), 'A usability checklist for the usability evaluation of mobile phone user interface', *International Journal of Human–Computer Interaction* **20**(3), 207–231. doi: 10.1207/s15327590ijhc2003_3.

Zirjawi, N., Kurtanovic, Z. & Maalej, W. (2015), A survey about user requirements for biometric authentication on smartphones, *in* '*2015 IEEE 2nd Workshop on Evolving Security and Privacy Requirements Engineering (ESPRE)*', pp. 1–6. doi: 10.1109/ESPRE.2015.7330160.

7 The relationship between usability and biometric authentication in mobile phones

Abstract. It is estimated that over 1 billion people are active mobile phone users in 2018. When using a mobile phone, there are a variety of ways to authenticate and "secure" the device, and biometric authentication is becoming an increasingly common way to do this, however, biometric authentication is not always as usable as it could be. Both usability and security are important, yet many people believe that there is a trade-off between the two. The focus of this paper was to better understand usability, computer security, and within computer security more specifically biometric authentication, and how all three can work together to create systems that are both usable and secure. A survey and interviews were conducted based on previous research to understand perceptions from the general population, usability experts, and security/biometrics experts. The results do indicate that there is indeed a perceived trade-off between usability and computer security.

Keywords: Usability, biometrics, authentication, security, mobile phone, user experience, computer security.

7.1 Introduction

Both usability and computer security are important, yet many people believe that there is a trade-off between the two [1, 12, 15]. A device that isn't usable won't be used, and if a device isn't secure, then it will be rendered useless [1]. This can often be seen with regards to mobile phones. With mobile phones being accessed and used by so many people, sometimes over 100 times a day [2], it is vital for these devices to have authentication methods that are both secure and usable. Biometric authentication is a growing option; however, it is not as widely adopted as many had thought it would be. Many people still rely on passwords, pins, patterns, or no authentication method because these are the methods they are used to. The problem that comes with these methods is that often, they are not very secure. Patterns leave smudges on screens, pins and passwords are often only a couple of digits or letters, and no authentication is an easy option. Biometric authentication could solve these problems. In theory, biometrics are both secure and usable, however in practice this is not always the case. Thus, it is important to understand how we can increase the usability and security of biometric authentication together so that there is a stronger option for securing mobile phones.

7.2 Background

7.2.1 A trade-off between usability and security?

When computers were first built, they were predominantly used by experts, so security was a concern, not usability. Now with computers ranging in sizes, functions, and being used by millions of people, usability as well as security are important concerns. If it is not usable, it won't be used, and if it's not secure, then it will become useless [1]. There has been debate as to whether there is a trade-off between security and usability. Some research has stated that there is a trade-off showing that usability reduces security [10], that usability and security have different goals [14], or that this trade-off poses serious problems for system designers [15]. However, a majority of research today seems to go the other way; it pre-dominantly depends on how security and usability are integrated into systems. The "'received wisdom' on the inherent conflict between usability and security goes against common sense" [1].

Discussions surrounding a trade-off between usability and security are often shallow [11]. There isn't discussion on the level of security that will be obtained and how usability will "hurt it" [11]. But usability can improve security. When usability and security are both incorporated into the design process, they can have the same goals [12]. And with an increased focus on users, there has been more research on the usability of security systems. Users make errors, so systems need to be designed to be either insensitive to those errors, to use metaphors and such to allow users to use security software more intuitively or provide users with the knowledge needed to make informed decisions [1]. When a system can interpret user desires correctly, then usability and security are working in harmony [12].

One problem that seems to arise is with the word "trade-off" itself. The way that security and usability are viewed must be changed and not thought of as a trade-off. When they are not integrated into the design process and are only seen as features, then there will of course be a trade-off. However, when viewed as qualities instead of features and are integrated into the design and development process, the perceived "trade-off" between usability and security can be reduced [12].

7.2.2 Biometric security

Biometric authentication is about authenticating a person for who they are, not by what they remember or what they have with them [13]. It can be a more long-term and cost-efficient authentication method, and in theory it should be both secure and usable [17]. This is not always the case though. Each biometric trait has their own pros and cons, and some issues that can come up with biometrics are noise, distinctiveness, and non-universality [13,17]. These issues can cause problems in the enrollment and authentication modes [13].

A few errors that can arise in the enrollment and authentication modes are failure to enroll (due to noise, distinctiveness, or not being able to use a specific biometric trait), false acceptance rate (accepting a non-match as a match), and false rejection rate (not accepting the enrolled trait) [19]. These errors can greatly influence the usability of a mobile phone, and a balance is needed between the usability and security [16]. It is crucial when it comes to user safety; however, user interfaces for authentication often encourage either secure or insecure behavior depending on its security requirements [16].

7.2.3 Usability and biometric authentication in mobile phones

Usability issues arise from a variety of sources. One large usability issue with regards to biometric authentication can come from the detection error trade-off curve. Unlike passwords, pins, and patterns that are either 100% correct or not, biometrics are based on how close of a match it is to the collected template from the enrollment mode [19]. The threshold that has been established will decide if the biometric is to be accepted or not. The accuracy and thresholds in biometric authentication do not always relate to the ease of use or convenience that users are used to and are looking for [19].

Some people believe that biometrics are not the default authentication mode due to usability and user experience [18]. Many users have not experienced a noticeable difference when using biometrics than using the authentication methods they have already been using [18]. A very common problem with usability in biometric authentication systems is that those who create a system or design of-ten think that it is intuitive and that users will easily understand; that is rarely the case. There is almost nothing that is inherently usable, and biometrics is no exception [19]. That is why biometric authentication systems should be designed with usability and security in mind throughout the whole design and development process [10, 11, 16].

7.3 Methodology

An explanatory research design was followed by using a survey in phase 1 fol-lowed by interviews in phase 2. As most research on biometric authentication and usability in mobile phones has focused on the general population, the goal here was to gather data on perceptions of biometric authentication and usability not just from the general population, but also from those who work in or with usability, computer security, and within that biometrics in particular. To accomplish this, survey and interview methods were used. The first phase consisted of the survey which had three user groups: the general population, usability experts, and computer security/ biometrics experts. The second phase consisted of inter-views with usability experts and computer security/ biometrics experts for more in-depth data collection based on the survey and its results. A majority of the survey questions were based on research previously conducted.

Questions such as gender [4, 6, 7], age [4, 5, 6, 7, 9], education level [6], knowledge about biometrics and usability [6, 4, 7], usability perceptions of bio-metrics [4], ease of use as well as security of biometrics [4, 5], operating system [8, 9], security tools (or authentication methods) used [8, 9], convenience [8, 5, 7], frequency of authentication [8], experience with failure to authenticate [8], and why participants use biometric authentication or not [7, 9] were used in the survey.

The survey design ensures potential bias is minimal. Before conducting phase 1 and 2, pilot tests were conducted on both the survey and the interview questions. To recruit participants for the survey and interviews, multiple channels were used. They can also be characterized convenience sampling. The survey was posted on multiple usability, design, computer security, and biometrics forums, Facebook groups, and LinkedIn groups. Also, 250 emails were sent to usability, design, computer security, and biometrics companies across 10+ countries to find more diverse participants.

7.4 Results

7.4.1 Survey results

24% of participants work in biometrics, security, or related fields. 31% of participants work in usability, UX, UI, or related fields. The remaining 45% of participants worked in neither of those areas. 96% of participants in this study use some form of authentication for unlocking their device, 75% of whom have had issues with unlocking their phones. Those who work in usability, security, or related fields tended to say that biometrics were the most secure and easy to use authentication method (86% and 83% respectively) however, only 67% of those who worked in neither of those areas chose biometrics as the most secure or easy to use authentication method. Those working in security or related fields believed in a link (96%) and trade-off (65%) between usability and security at a much higher level than the other two participant groups (80% and 50% for usability participants respectively and 63% and 47% of general participants respectively). The percentage of participants who were uncertain if there was a link or a trade-off between security and usability increased from security participants (0% were uncertain of there being a link and 13% for a trade-off), to usability participants (3% were uncertain of there being a link and 17% for a trade-off), to general participants (28% were uncertain of there being a link and 37% for a trade-off). However, across the board, a majority of participants (63%) believe that mobile phones can be secure and usable, but they are not always like that today. When asked about their understanding of biometrics, the average understanding was a 3 on a scale of 1-6. 53% of general participants said that they had little to no understanding of biometrics, 60% of usability participants said that they had a nov-ice to intermediate understanding of biometrics, and 57% of biometrics participants said that they have an advanced or expert understanding. When asked about their understanding of usability, the average understanding was a 4 on a scale of 1-6. 44% of general participants said that they had a novice to intermediate understanding of usability, 48% of security participants said that they had an advanced or expert understanding of usability, and 70% of usability participants said that they had an advanced or expert understanding of usability. 83% of security participants said that they have worked with usability experts whereas only 33% of usability experts said that they have worked with security experts.

There was a high correlation between participants who use a particular well-known brand of mobile phones and use of biometrics (94%) and having the belief that biometrics are the most secure and easy to use authentication method. A majority of participants whose age was between 35-44 years old use biometrics (90%) and had perceptions of biometrics being the most secure

(85%) and easy to use (91%) authentication method. 100% of participants over the age of 45 said that biometrics are the most secure and easy to use authentication method. Over-all, as the understanding of biometrics and usability increased, so did the belief of a link between the two increase.

7.4.2 Interview results

One common theme that emerged from the interviews was about users of mobile phones. Several participants discussed how everything "goes back to the user" and how there is much that "depends on the person". These users discussed how users "shouldn't be locked into letting go of something or using something specifically", and that users will disable or circumvent security measures. Many people use the same passwords or pins "as their default method because they are used to it". Security measures now often depend on "what people are willing to do" or "what effort people are willing to make".

Another common theme that emerged was about the weaknesses of security in mobile phones. Multiple participants discussed margins of error, type I and type II errors, and how information is sent mainly around biometric authentication. When discussing the weaknesses of biometric authentication specifically, one participant said, "theoretically it can work and [security] can increase, but in practice it hasn't been that way", and another said that "when it comes down to it, it can be done, but at a cost". Another participant discussed how "you can use a backup method as heightened security, but... the methods used as a backup aren't secure methods".

In five of the six interviews when it came to the question about there being a trade-off or not between usability and security, it was mentioned that there needs to be a balance between usability and security; and even though there is a trade-off, it is not necessarily a bad thing or a problem. Another specific point that was discussed with four of the six participants was 2-factor authentication. Some of these participants mentioned how some data is stored due to two-factor authentication or that it is often recommended for heightened security, though it may be "overboard" or "not always practical for the end user".

There were a few phrases that participants said that were important to them. "Usability is the reason why biometrics are used". "Authentication needs to just work". "UX should not interrupt security". "Bigger phones" reduce the number of usable methods for authentication, although it was not clear what they meant by “bigger phones”. "There needs to be an explanation to the user". "Independent testing is so important". "There needs to be a way to protect the device even when there is no physical access to it". "There is always the question about what is the best option today".

7.5 Discussion

In general, the survey results showed corroboration with what [8], [3], and [5] stated in that overall there is a belief outside of the security profession that security is important.

Similar to what [3], 76% of participants said that biometrics were the most secure authentication option followed by pins and passwords (22%).

As the other studies mentioned showed as well, fingerprint authentication was the most preferred and used biometric.

Something that was noticed during data analysis was about perceptions and understanding of usability. There were more people than expected outside of the field of usability who said that they have an advanced or expert understanding of usability, and this could be due to the simple definition of usability provided in the survey.

Throughout the interviews there were some common factors that came up. Participants discussed how usability is a large reason as to why biometric authentication is used, and as of now there is a lot of variation between biometric authentication methods and their levels of usability. Humans are an important factor that are often overlooked or thought of as a problem when it comes to authentication. Several participants also mentioned how if security is not usable, then users will circumvent it. Usability should not get in the way of security and vice versa. It was also discussed how there is a trade-off between usability and security, however that it may not necessarily be a problem to have that trade-off. Perhaps by saying it is not a problem the users imply that a healthy balance can be reached through good design between a desirable level of usability and computer security.

7.6 Conclusion

All groups of users see a link between usability and computer security (specifically with biometric authentication). All groups of users see a trade-off between them and simultaneously believe that an optimum level of both is possible through good mobile phone design.

7.6.1 Future work

As of now we do not know exactly how the trade-off between usability and computer security manifests itself. We need to establish that they are related through objective data. As of now we have concluded the link based on subjective self-reported data from three categories of users. The interviews bring up several good hypotheses for future usability and computer security studies but each of them needs to be investigated in greater detail so that there are findings that can be in the form of clear design guidelines.

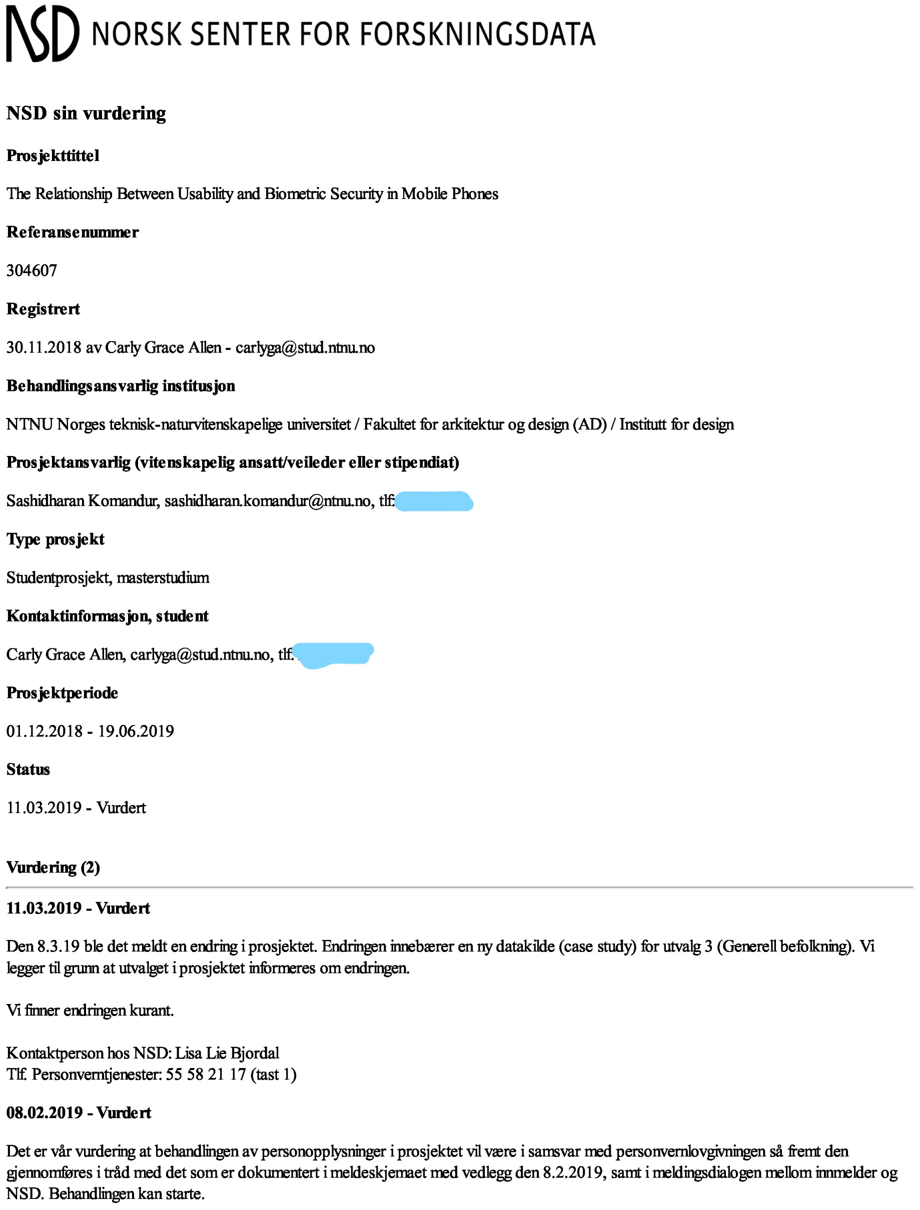
7.7 References

1. Cranor, L. and Garfinkel, S.: Guest editors' introduction: Secure or usable? Security & Privacy, IEEE 2(5), 16-18 (2004).
2. Griffin, A.: iPhones are unlocked 80 times per day, Apple says as part of security brief-ing, The Independent UK (2016).
3. Zirjawi, N., Kurtanovic, Z. and Maalej, W.: A survey about user requirements for bio-metric authentication on smartphones, 2015 IEEE 2nd Workshop on Evolving Security and PrivacyRequirements Engineering (ESPRE), 1-6 (2015).

4. Riley, C.W., Buckner, K., Johnson, G. and Benyon, D.: Culture & biometrics: regional differences in the perception of biometric authentication technologies. AI & Soc, 295-306 (2008).
5. Lovisotto, G., Malik, R., Sluganovic, I., Roeschlin, M., Trueman, P. and Martinovic, I.: Mobile Biometrics in Financial Services: A Five Factor Framework. University of Ox-ford (2017).
6. El-Abed, M., Giot, R., Hemery, B. and Rosenberger, C.: A study of users' acceptance and satisfaction of biometric systems. 44th Annual 2010 IEEE International Carnahan Conference on Security Technology, 170-178 (2010).
7. Bhagavatula, C., Ur, B., Lacovino, K., Mon Kywe, S., Cranor, L., and Savvides, M.: Biometric authentication on iphone and android: Usability, perceptions, and influences on adoption. Workshop on Usable Security at USEC '15 (2015).
8. Al Abdulwahid, A., Clarke, N., Stengel, I., Furnell, S. and Reich, C.: Security, privacy, and usability – a survey of users' perceptions and attitudes. Trust, Privacy, and Securi-ty in Digital Business, 153-168 (2015).
9. Ahmed, I.U.: Smartphone Authentication, User experience, expectation and satisfaction. Master's Thesis (2017).
10. Alshamari, M.: A review of gaps between usability and security/privacy. International Journal of Communications, Network and System Sciences, 413-429 (2016).
11. Sasse, M.A., Smith, M., Herley, C., Lipford, H. and Vaniea, K.: Debunking Security-Usability Tradeoff Myths. IEEE Security Privacy (2016).
12. Yee, K.P.: Guidelines and Strategies for Secure Interaction Design. Usability and Secu-rity: Designing Secure Systems That People Can Use (2005).
13. Böhm, I. and Testor, F.: Biometric Systems. Department of Telecooperation University of Linz (2004).
14. Sahar, F.: Tradeoffs between Usability and Security. International Journal of Engineer-ing and Technology (2013).
15. Ben-Asher, N., Meyer, J., Möller, S. and Englert, R.: An Experimental System for Studying the Tradeoff between Usability and Security. 2009 International Conference on Availability, Reliability and Security (2009).
16. Oluwatosin Nwokedi ,U., Amunga, B. and Bashari Rad, B.: Usability and Security in User Interface Design: A Systematic Literature Review (2016).
17. Pocovnicu, A.: Biometric Security for Cell Phones. Informatica Economica (2009).
18. Brostoff, G.: Adoption problems? How UX could boost biometrics. Biometric Tech-nology Today (2017).
19. Coventry, L.: Usable Biometrics. Security and Usability: Designing Secure Systems that People Can Use (2005).

A Appendix

A.1 NSD approval - Norwegian



NSD NORSK SENTER FOR FORSKNINGSDATA

NSD sin vurdering

Prosjekttittel

The Relationship Between Usability and Biometric Security in Mobile Phones

Referansenummer

304607

Registrert

30.11.2018 av Carly Grace Allen - carlyga@stud.ntnu.no

Behandlingsansvarlig institusjon

NTNU Norges teknisk-naturvitenskapelige universitet / Fakultet for arkitektur og design (AD) / Institutt for design

Prosjektansvarlig (vitenskapelig ansatt/veileder eller stipendiat)

Sashidharan Komandur, sashidharan.komandur@ntnu.no, tlf: [redacted]

Type prosjekt

Studentprosjekt, masterstudium

Kontaktinformasjon, student

Carly Grace Allen, carlyga@stud.ntnu.no, tlf: [redacted]

Prosjektperiode

01.12.2018 - 19.06.2019

Status

11.03.2019 - Vurdert

Vurdering (2)

11.03.2019 - Vurdert

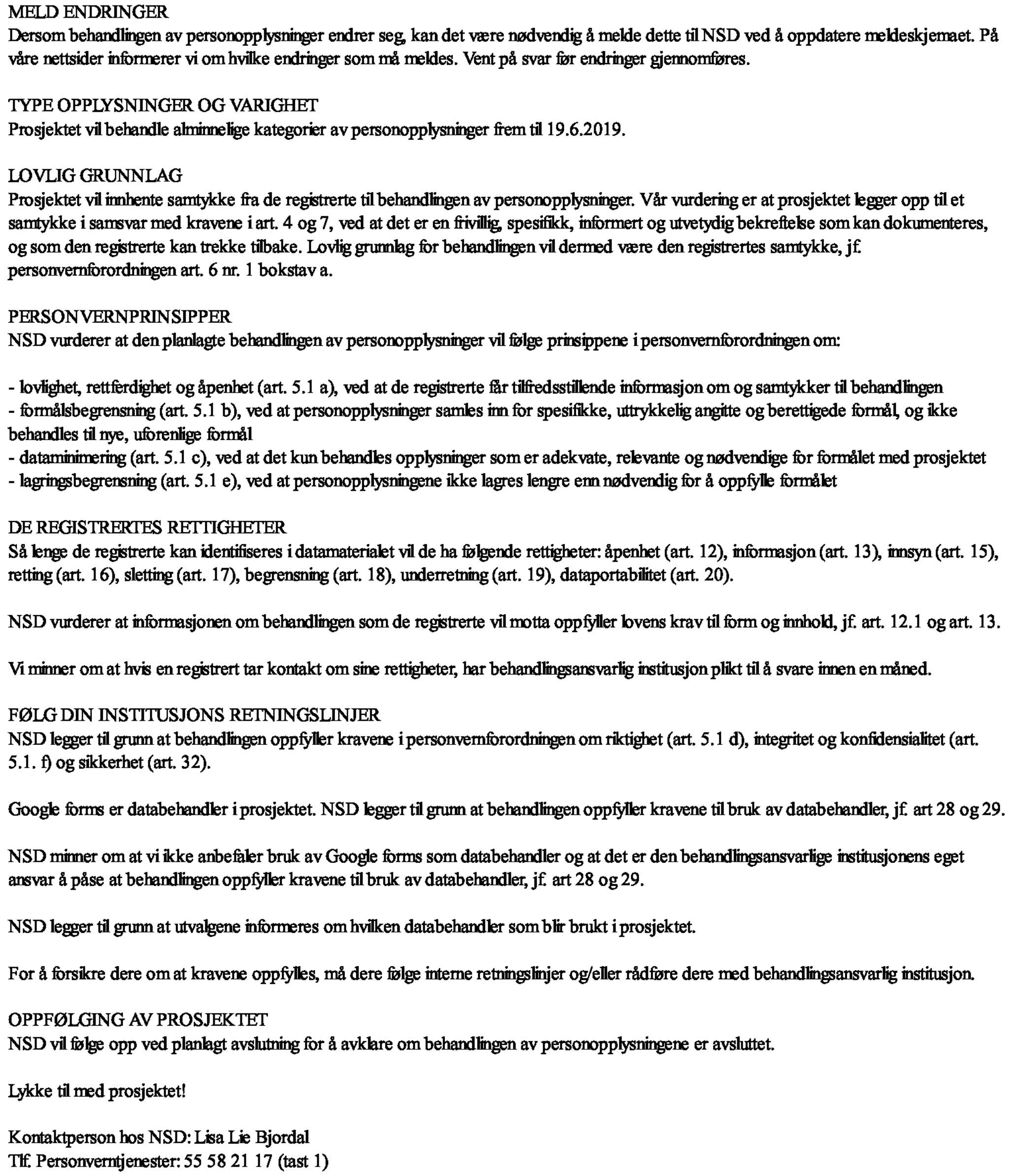
Den 8.3.19 ble det meldt en endring i prosjektet. Endringen innebærer en ny datakilde (case study) for utvalg 3 (Generell befolkning). Vi legger til grunn at utvalget i prosjektet informeres om endringen.

Vi finner endringen kurant.

Kontaktperson hos NSD: Lisa Lie Bjordal
Tlf. Personverntjenester: 55 58 21 17 (tast 1)

08.02.2019 - Vurdert

Det er vår vurdering at behandlingen av personopplysninger i prosjektet vil være i samsvar med personvernlovgivningen så fremt den gjennomføres i tråd med det som er dokumentert i meldeskjemaet med vedlegg den 8.2.2019, samt i meldingsdialogen mellom innmelder og NSD. Behandlingen kan starte.



MELD ENDRINGER
Dersom behandlingen av personopplysninger endrer seg, kan det være nødvendig å melde dette til NSD ved å oppdatere meldeskjemaet. På våre nettsider informerer vi om hvilke endringer som må meldes. Vent på svar før endringer gjennomføres.

TYPE OPPLYSNINGER OG VARIGHET
Prosjektet vil behandle alminnelige kategorier av personopplysninger frem til 19.6.2019.

LOVLIG GRUNNLAG
Prosjektet vil innhente samtykke fra de registrerte til behandlingen av personopplysninger. Vår vurdering er at prosjektet legger opp til et samtykke i samsvar med kravene i art. 4 og 7, ved at det er en frivillig, spesifikk, informert og utvetydig bekreftelse som kan dokumenteres, og som den registrerte kan trekke tilbake. Lovlig grunnlag for behandlingen vil dermed være den registrertes samtykke, jf. personvernforordningen art. 6 nr. 1 bokstav a.

PERSONVERNPRINSIPPER
NSD vurderer at den planlagte behandlingen av personopplysninger vil følge prinsippene i personvernforordningen om:

- lovlighet, rettferdighet og åpenhet (art. 5.1 a), ved at de registrerte får tilfredsstillende informasjon om og samtykker til behandlingen
- formålsbegrensning (art. 5.1 b), ved at personopplysninger samles inn for spesifikke, uttrykkelig angitte og berettigede formål, og ikke behandles til nye, uforenlige formål
- dataminimering (art. 5.1 c), ved at det kun behandles opplysninger som er adekvate, relevante og nødvendige for formålet med prosjektet
- lagringsbegrensning (art. 5.1 e), ved at personopplysningene ikke lagres lengre enn nødvendig for å oppfylle formålet

DE REGISTRERTES RETTIGHETER
Så lenge de registrerte kan identifiseres i datamaterialet vil de ha følgende rettigheter: åpenhet (art. 12), informasjon (art. 13), innsyn (art. 15), retting (art. 16), sletting (art. 17), begrensning (art. 18), underretning (art. 19), dataportabilitet (art. 20).

NSD vurderer at informasjonen om behandlingen som de registrerte vil motta oppfyller lovens krav til form og innhold, jf. art. 12.1 og art. 13.

Vi minner om at hvis en registrert tar kontakt om sine rettigheter, har behandlingsansvarlig institusjon plikt til å svare innen en måned.

FØLG DIN INSTITUSJONS RETNINGSLINJER
NSD legger til grunn at behandlingen oppfyller kravene i personvernforordningen om riktighet (art. 5.1 d), integritet og konfidensialitet (art. 5.1. f) og sikkerhet (art. 32).

Google forms er databehandler i prosjektet. NSD legger til grunn at behandlingen oppfyller kravene til bruk av databehandler, jf. art 28 og 29.

NSD minner om at vi ikke anbefaler bruk av Google forms som databehandler og at det er den behandlingsansvarlige institusjonens eget ansvar å påse at behandlingen oppfyller kravene til bruk av databehandler, jf. art 28 og 29.

NSD legger til grunn at utvalgene informeres om hvilken databehandler som blir brukt i prosjektet.

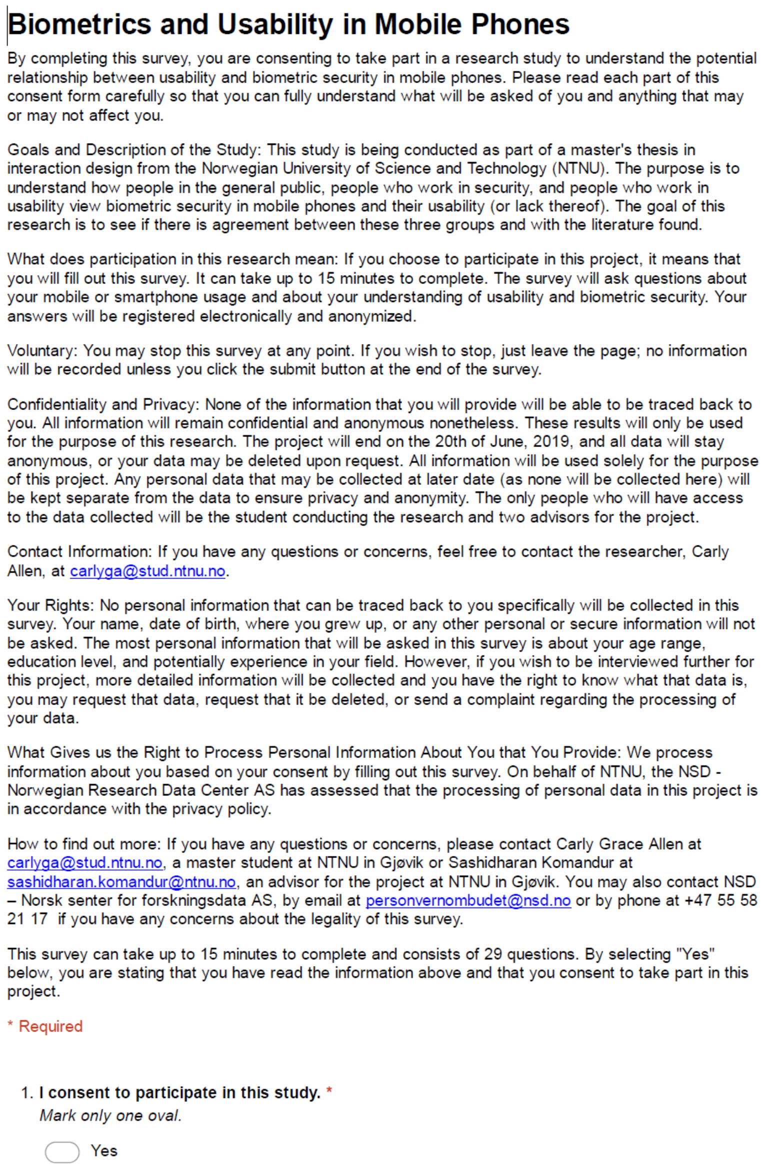
For å forsikre dere om at kravene oppfylles, må dere følge interne retningslinjer og/eller rådføre dere med behandlingsansvarlig institusjon.

OPPFØLGING AV PROSJEKTET
NSD vil følge opp ved planlagt avslutning for å avklare om behandlingen av personopplysningene er avsluttet.

Lykke til med prosjektet!

Kontaktperson hos NSD: Lisa Lie Bjordal
Tlf. Personverntjenester: 55 58 21 17 (tast 1)

A.2 Survey consent form



Biometrics and Usability in Mobile Phones

By completing this survey, you are consenting to take part in a research study to understand the potential relationship between usability and biometric security in mobile phones. Please read each part of this consent form carefully so that you can fully understand what will be asked of you and anything that may or may not affect you.

Goals and Description of the Study: This study is being conducted as part of a master's thesis in interaction design from the Norwegian University of Science and Technology (NTNU). The purpose is to understand how people in the general public, people who work in security, and people who work in usability view biometric security in mobile phones and their usability (or lack thereof). The goal of this research is to see if there is agreement between these three groups and with the literature found.

What does participation in this research mean: If you choose to participate in this project, it means that you will fill out this survey. It can take up to 15 minutes to complete. The survey will ask questions about your mobile or smartphone usage and about your understanding of usability and biometric security. Your answers will be registered electronically and anonymized.

Voluntary: You may stop this survey at any point. If you wish to stop, just leave the page; no information will be recorded unless you click the submit button at the end of the survey.

Confidentiality and Privacy: None of the information that you will provide will be able to be traced back to you. All information will remain confidential and anonymous nonetheless. These results will only be used for the purpose of this research. The project will end on the 20th of June, 2019, and all data will stay anonymous, or your data may be deleted upon request. All information will be used solely for the purpose of this project. Any personal data that may be collected at later date (as none will be collected here) will be kept separate from the data to ensure privacy and anonymity. The only people who will have access to the data collected will be the student conducting the research and two advisors for the project.

Contact Information: If you have any questions or concerns, feel free to contact the researcher, Carly Allen, at carlyga@stud.ntnu.no.

Your Rights: No personal information that can be traced back to you specifically will be collected in this survey. Your name, date of birth, where you grew up, or any other personal or secure information will not be asked. The most personal information that will be asked in this survey is about your age range, education level, and potentially experience in your field. However, if you wish to be interviewed further for this project, more detailed information will be collected and you have the right to know what that data is, you may request that data, request that it be deleted, or send a complaint regarding the processing of your data.

What Gives us the Right to Process Personal Information About You that You Provide: We process information about you based on your consent by filling out this survey. On behalf of NTNU, the NSD - Norwegian Research Data Center AS has assessed that the processing of personal data in this project is in accordance with the privacy policy.

How to find out more: If you have any questions or concerns, please contact Carly Grace Allen at carlyga@stud.ntnu.no, a master student at NTNU in Gjøvik or Sashidharan Komandur at sashidharan.komandur@ntnu.no, an advisor for the project at NTNU in Gjøvik. You may also contact NSD – Norsk senter for forskningsdata AS, by email at personvernombudet@nsd.no or by phone at +47 55 58 21 17 if you have any concerns about the legality of this survey.

This survey can take up to 15 minutes to complete and consists of 29 questions. By selecting "Yes" below, you are stating that you have read the information above and that you consent to take part in this project.

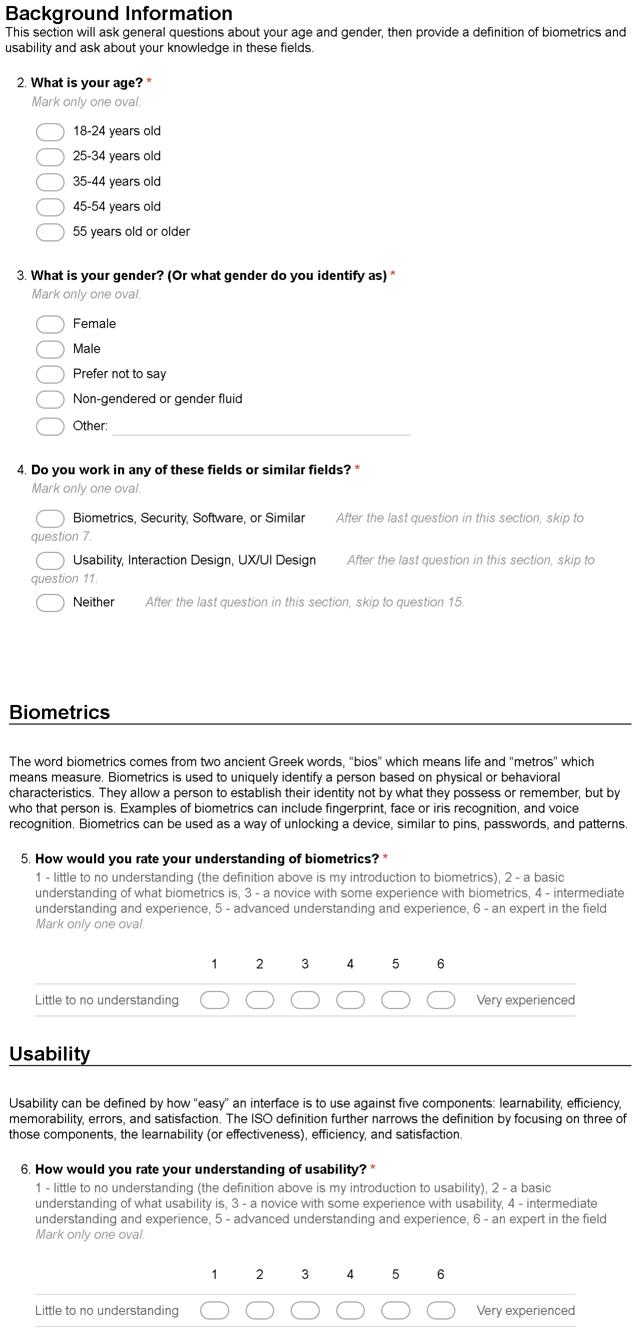
* Required

1. **I consent to participate in this study.** *

Mark only one oval.

○ Yes

A.3 Survey questionnaire



Background Information

This section will ask general questions about your age and gender, then provide a definition of biometrics and usability and ask about your knowledge in these fields.

2. **What is your age?** *

Mark only one oval.

○ 18-24 years old
○ 25-34 years old
○ 35-44 years old
○ 45-54 years old
○ 55 years old or older

3. **What is your gender? (Or what gender do you identify as)** *

Mark only one oval.

○ Female
○ Male
○ Prefer not to say
○ Non-gendered or gender fluid
○ Other: ____________________

4. **Do you work in any of these fields or similar fields?** *

Mark only one oval.

○ Biometrics, Security, Software, or Similar *After the last question in this section, skip to question 7.*
○ Usability, Interaction Design, UX/UI Design *After the last question in this section, skip to question 11.*
○ Neither *After the last question in this section, skip to question 15.*

Biometrics

The word biometrics comes from two ancient Greek words, "bios" which means life and "metros" which means measure. Biometrics is used to uniquely identify a person based on physical or behavioral characteristics. They allow a person to establish their identity not by what they possess or remember, but by who that person is. Examples of biometrics can include fingerprint, face or iris recognition, and voice recognition. Biometrics can be used as a way of unlocking a device, similar to pins, passwords, and patterns.

5. **How would you rate your understanding of biometrics?** *

1 - little to no understanding (the definition above is my introduction to biometrics), 2 - a basic understanding of what biometrics is, 3 - a novice with some experience with biometrics, 4 - intermediate understanding and experience, 5 - advanced understanding and experience, 6 - an expert in the field

Mark only one oval.

	1	2	3	4	5	6	
Little to no understanding	○	○	○	○	○	○	Very experienced

Usability

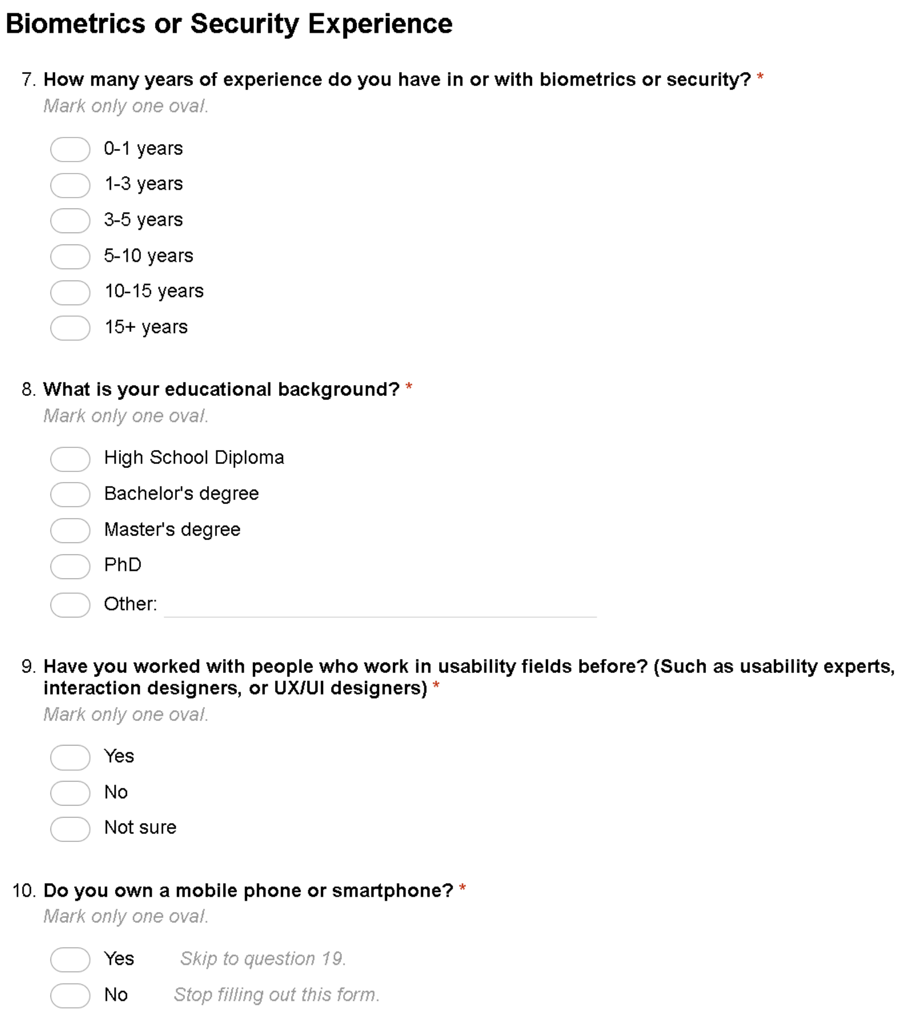
Usability can be defined by how "easy" an interface is to use against five components: learnability, efficiency, memorability, errors, and satisfaction. The ISO definition further narrows the definition by focusing on three of those components, the learnability (or effectiveness), efficiency, and satisfaction.

6. **How would you rate your understanding of usability?** *

1 - little to no understanding (the definition above is my introduction to usability), 2 - a basic understanding of what usability is, 3 - a novice with some experience with usability, 4 - intermediate understanding and experience, 5 - advanced understanding and experience, 6 - an expert in the field

Mark only one oval.

	1	2	3	4	5	6	
Little to no understanding	○	○	○	○	○	○	Very experienced



Biometrics or Security Experience

7. **How many years of experience do you have in or with biometrics or security?** *

Mark only one oval.

○ 0-1 years
○ 1-3 years
○ 3-5 years
○ 5-10 years
○ 10-15 years
○ 15+ years

8. **What is your educational background?** *

Mark only one oval.

○ High School Diploma
○ Bachelor's degree
○ Master's degree
○ PhD
○ Other: ____________________

9. **Have you worked with people who work in usability fields before? (Such as usability experts, interaction designers, or UX/UI designers)** *

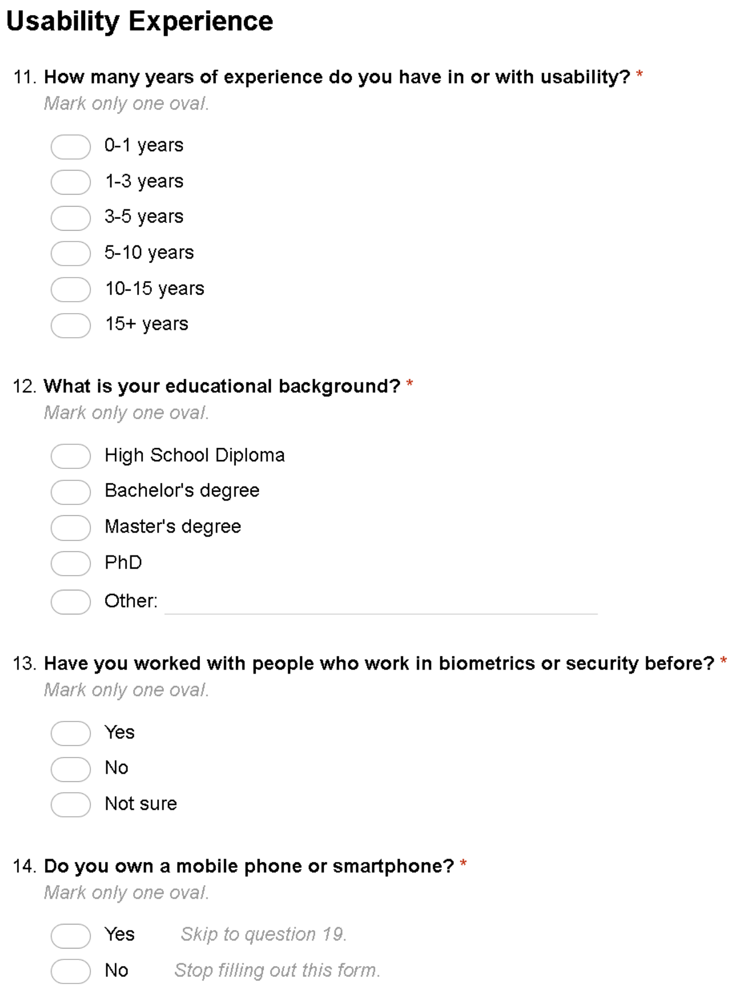
Mark only one oval.

○ Yes
○ No
○ Not sure

10. **Do you own a mobile phone or smartphone?** *

Mark only one oval.

○ Yes *Skip to question 19.*
○ No *Stop filling out this form.*



Usability Experience

11. **How many years of experience do you have in or with usability?** *

Mark only one oval.

○ 0-1 years
○ 1-3 years
○ 3-5 years
○ 5-10 years
○ 10-15 years
○ 15+ years

12. **What is your educational background?** *

Mark only one oval.

○ High School Diploma
○ Bachelor's degree
○ Master's degree
○ PhD
○ Other: ____________________

13. **Have you worked with people who work in biometrics or security before?** *

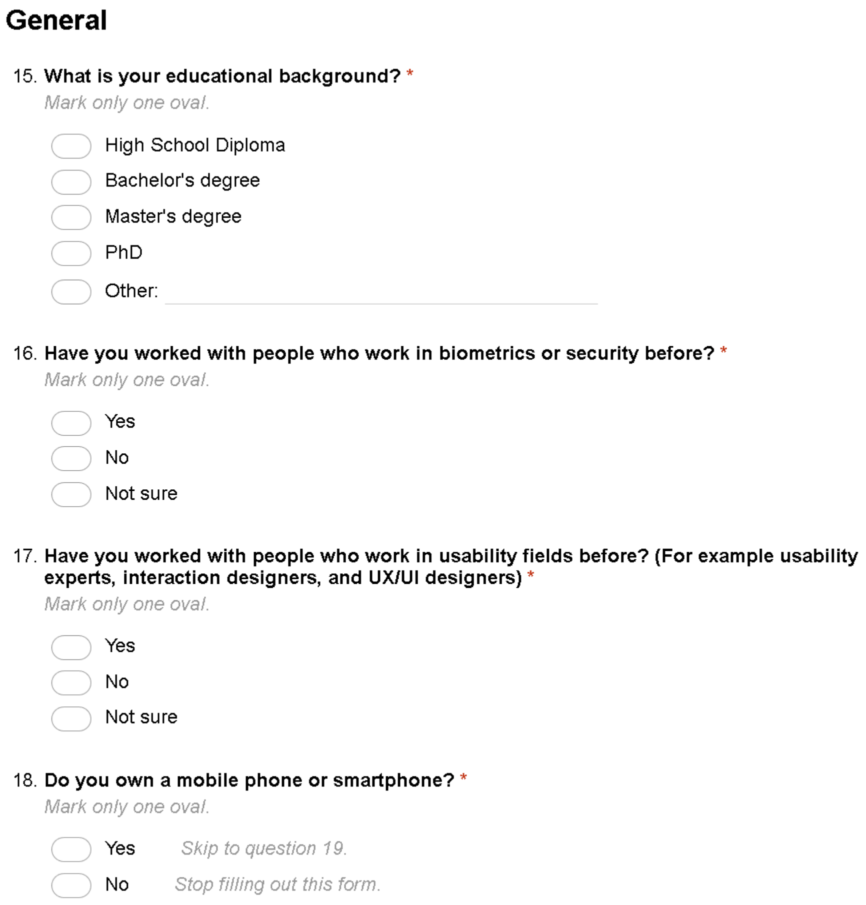
Mark only one oval.

○ Yes
○ No
○ Not sure

14. **Do you own a mobile phone or smartphone?** *

Mark only one oval.

○ Yes *Skip to question 19.*
○ No *Stop filling out this form.*



General

15. **What is your educational background?** *

Mark only one oval.

○ High School Diploma
○ Bachelor's degree
○ Master's degree
○ PhD
○ Other: ____________________

16. **Have you worked with people who work in biometrics or security before?** *

Mark only one oval.

○ Yes
○ No
○ Not sure

17. **Have you worked with people who work in usability fields before? (For example usability experts, interaction designers, and UX/UI designers)** *

Mark only one oval.

○ Yes
○ No
○ Not sure

18. **Do you own a mobile phone or smartphone?** *

Mark only one oval.

○ Yes *Skip to question 19.*
○ No *Stop filling out this form.*

Mobile Phone/Smartphone Usage

The questions in this section will ask about mobile phone or smartphone usage.

19. **How often do you unlock your phone? (Make a rough estimate)** *

Mark only one oval.

○ Seldom
○ Occasionally (a few times a month)
○ Often (a few times a week)
○ A few times a day
○ 10-20 times a day
○ 20-50 times a day
○ 50+ times a day

20. **What brand of mobile phone or smartphone do you own or primarily use?** *

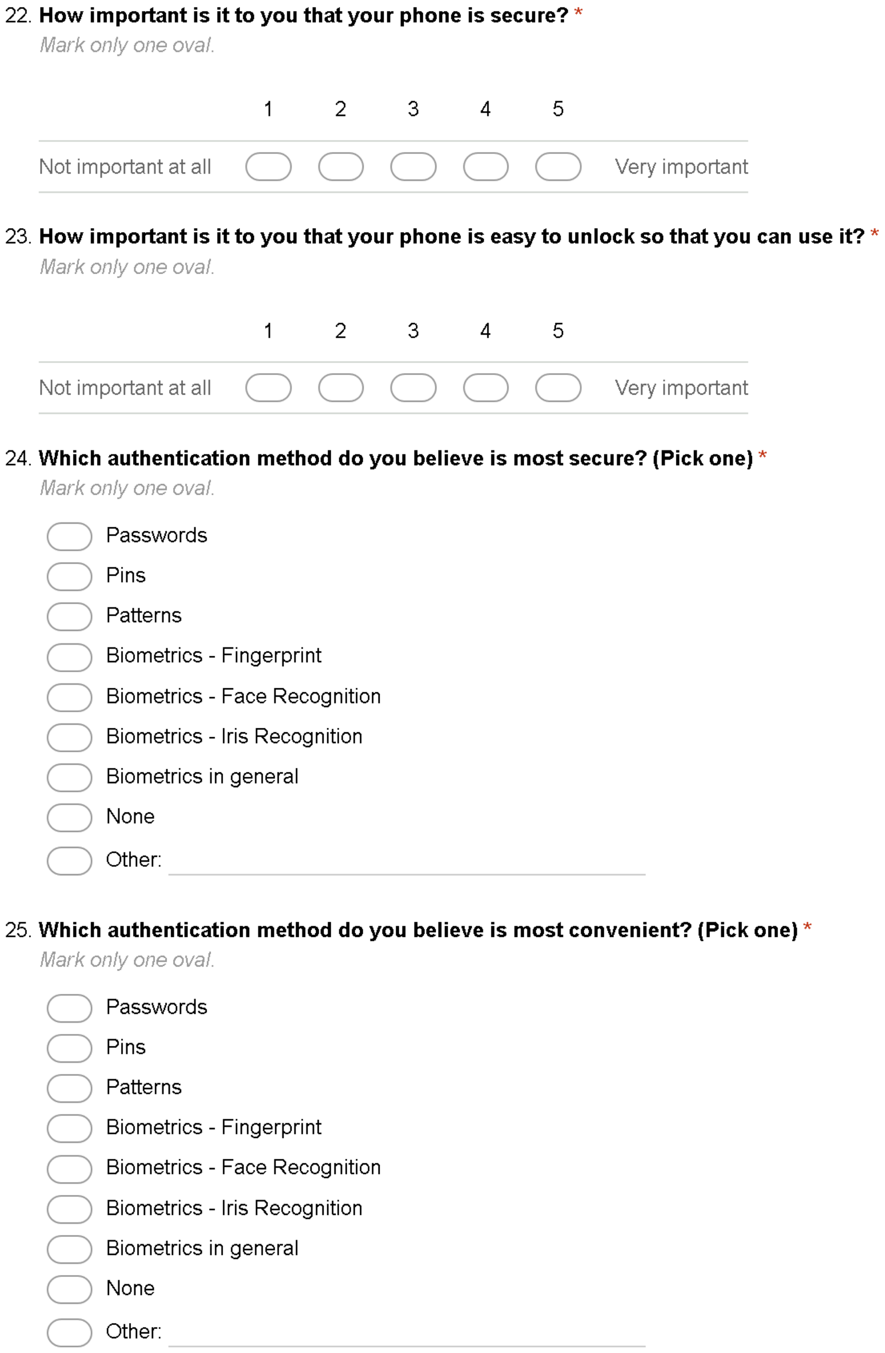
Mark only one oval.

○ Apple
○ Samsung
○ Huawei
○ Nokia
○ Sony
○ LG
○ HTC
○ Motorola
○ Blackberry
○ Other: ____________________

21. **Do you use an authentication method to unlock your phone? (And if so, the primary method that you use)** *

Mark only one oval.

○ Yes - Password
○ Yes - Pin
○ Yes - Pattern
○ Yes - Fingerprint recognition
○ Yes - Face recognition
○ Yes - iris recognition
○ Yes - another biometric or combination of biometrics
○ No - No authentication method at all
○ Other: ____________________



22. **How important is it to you that your phone is secure?** *

Mark only one oval.

	1	2	3	4	5	
Not important at all	○	○	○	○	○	Very important

23. **How important is it to you that your phone is easy to unlock so that you can use it?** *

Mark only one oval.

	1	2	3	4	5	
Not important at all	○	○	○	○	○	Very important

24. **Which authentication method do you believe is most secure? (Pick one)** *

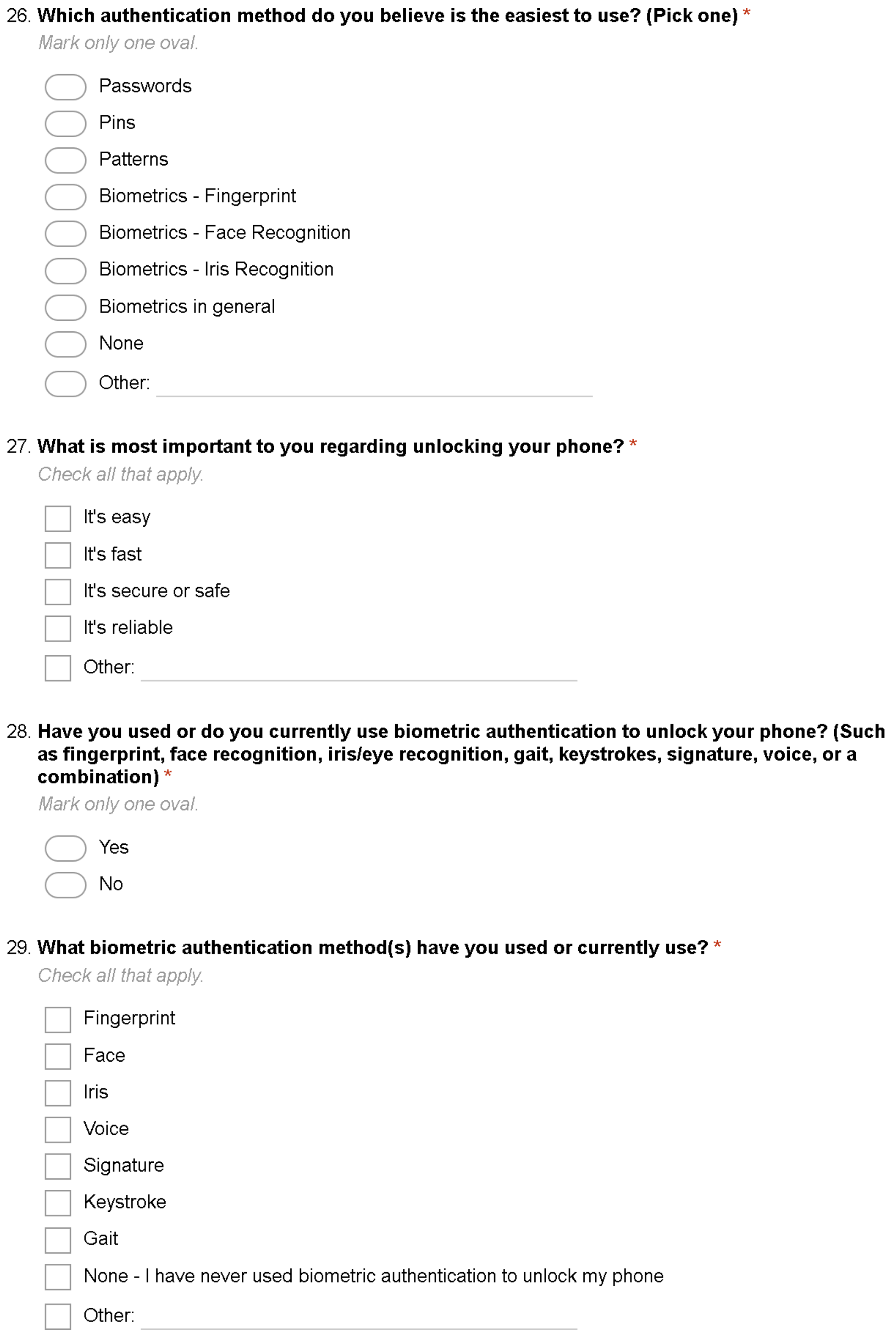
Mark only one oval.

○ Passwords
○ Pins
○ Patterns
○ Biometrics - Fingerprint
○ Biometrics - Face Recognition
○ Biometrics - Iris Recognition
○ Biometrics in general
○ None
○ Other: ______________________

25. **Which authentication method do you believe is most convenient? (Pick one)** *

Mark only one oval.

○ Passwords
○ Pins
○ Patterns
○ Biometrics - Fingerprint
○ Biometrics - Face Recognition
○ Biometrics - Iris Recognition
○ Biometrics in general
○ None
○ Other: ______________________



26. **Which authentication method do you believe is the easiest to use? (Pick one)** *

Mark only one oval.

○ Passwords
○ Pins
○ Patterns
○ Biometrics - Fingerprint
○ Biometrics - Face Recognition
○ Biometrics - Iris Recognition
○ Biometrics in general
○ None
○ Other: ______________________

27. **What is most important to you regarding unlocking your phone?** *

Check all that apply.

□ It's easy
□ It's fast
□ It's secure or safe
□ It's reliable
□ Other: ______________________

28. **Have you used or do you currently use biometric authentication to unlock your phone? (Such as fingerprint, face recognition, iris/eye recognition, gait, keystrokes, signature, voice, or a combination)** *

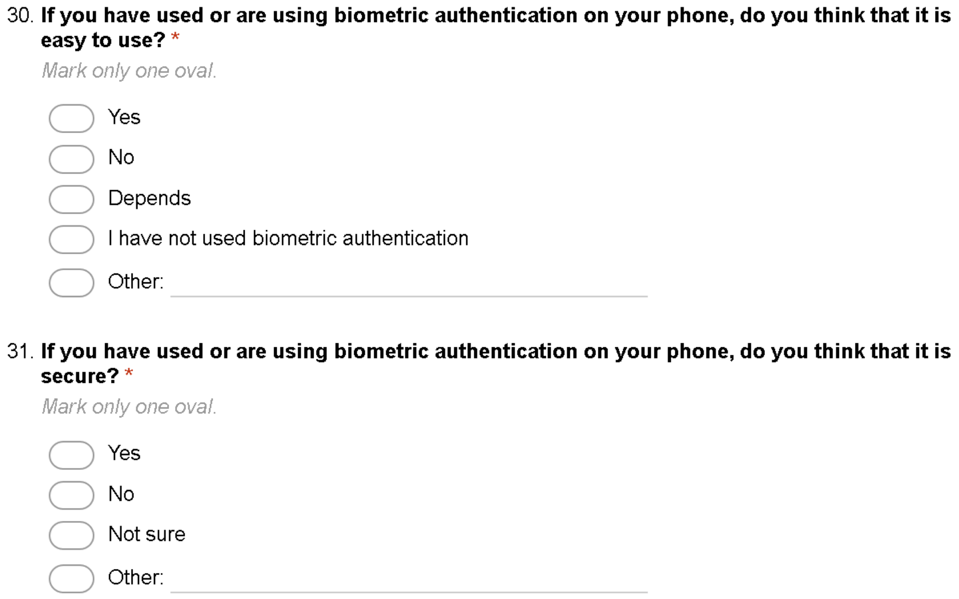
Mark only one oval.

○ Yes
○ No

29. **What biometric authentication method(s) have you used or currently use?** *

Check all that apply.

□ Fingerprint
□ Face
□ Iris
□ Voice
□ Signature
□ Keystroke
□ Gait
□ None - I have never used biometric authentication to unlock my phone
□ Other: ______________________



30. **If you have used or are using biometric authentication on your phone, do you think that it is easy to use?** *

Mark only one oval.

○ Yes

○ No

○ Depends

○ I have not used biometric authentication

○ Other: ______________________

31. **If you have used or are using biometric authentication on your phone, do you think that it is secure?** *

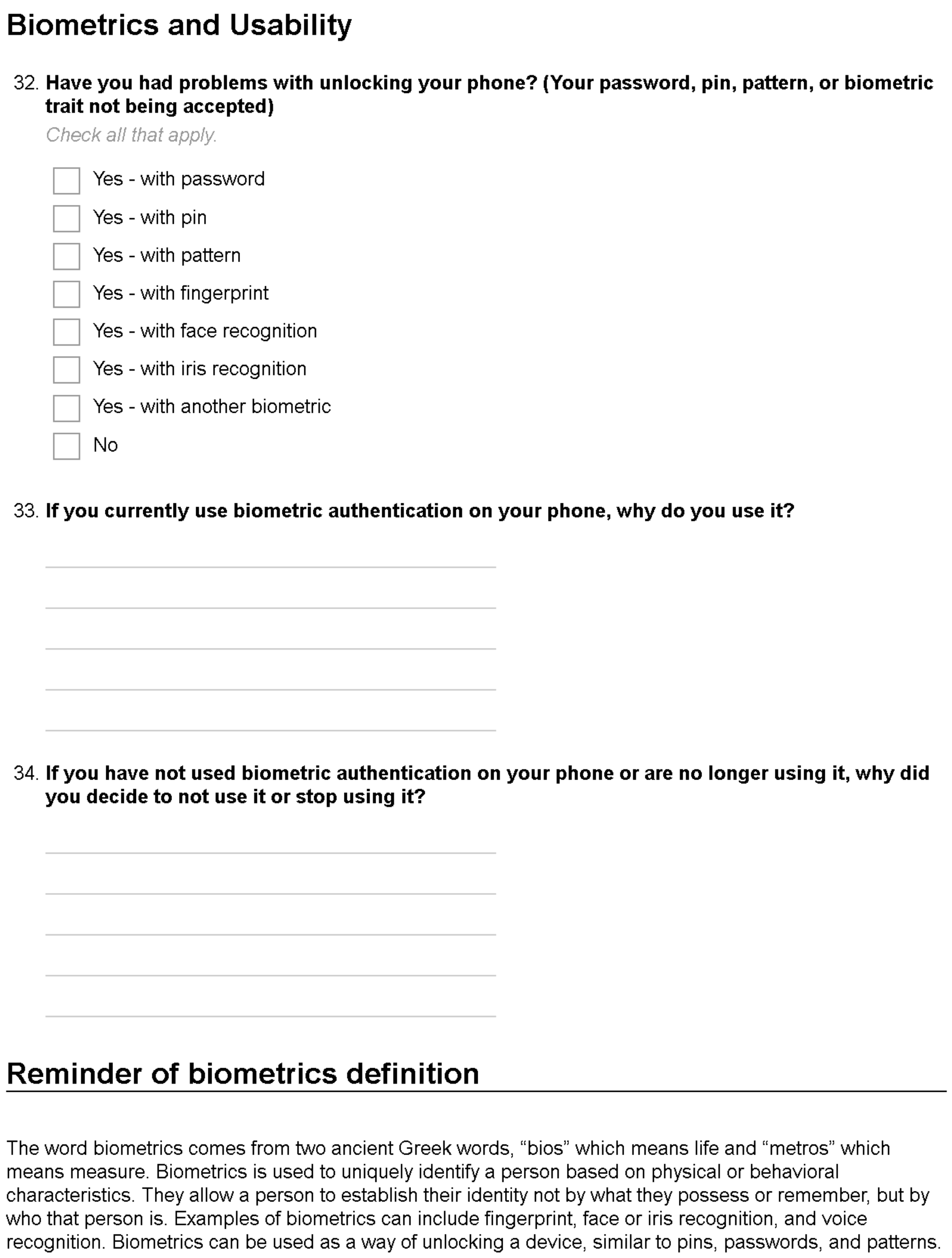
Mark only one oval.

○ Yes

○ No

○ Not sure

○ Other: ______________________



Biometrics and Usability

32. **Have you had problems with unlocking your phone? (Your password, pin, pattern, or biometric trait not being accepted)**

Check all that apply.

□ Yes - with password
□ Yes - with pin
□ Yes - with pattern
□ Yes - with fingerprint
□ Yes - with face recognition
□ Yes - with iris recognition
□ Yes - with another biometric
□ No

33. **If you currently use biometric authentication on your phone, why do you use it?**

34. **If you have not used biometric authentication on your phone or are no longer using it, why did you decide to not use it or stop using it?**

Reminder of biometrics definition

The word biometrics comes from two ancient Greek words, “bios” which means life and “metros” which means measure. Biometrics is used to uniquely identify a person based on physical or behavioral characteristics. They allow a person to establish their identity not by what they possess or remember, but by who that person is. Examples of biometrics can include fingerprint, face or iris recognition, and voice recognition. Biometrics can be used as a way of unlocking a device, similar to pins, passwords, and patterns.

Reminder of usability definition

Usability can be defined by how “easy” an interface is to use against five components: learnability, efficiency, memorability, errors, and satisfaction. The ISO definition further narrows the definition by focusing on three of those components, the learnability (or effectiveness), efficiency, and satisfaction.

35. **Do you believe that there is a link between security and usability?** *

Mark only one oval.

○ Yes
○ No
○ Maybe, not sure

36. **Do you believe that there is a trade-off between security and usability? (Does one increase while the other decreases)** *

Mark only one oval.

○ Yes
○ No
○ Maybe, not sure

37. **Please select which option you most believe:** *

Mark only one oval.

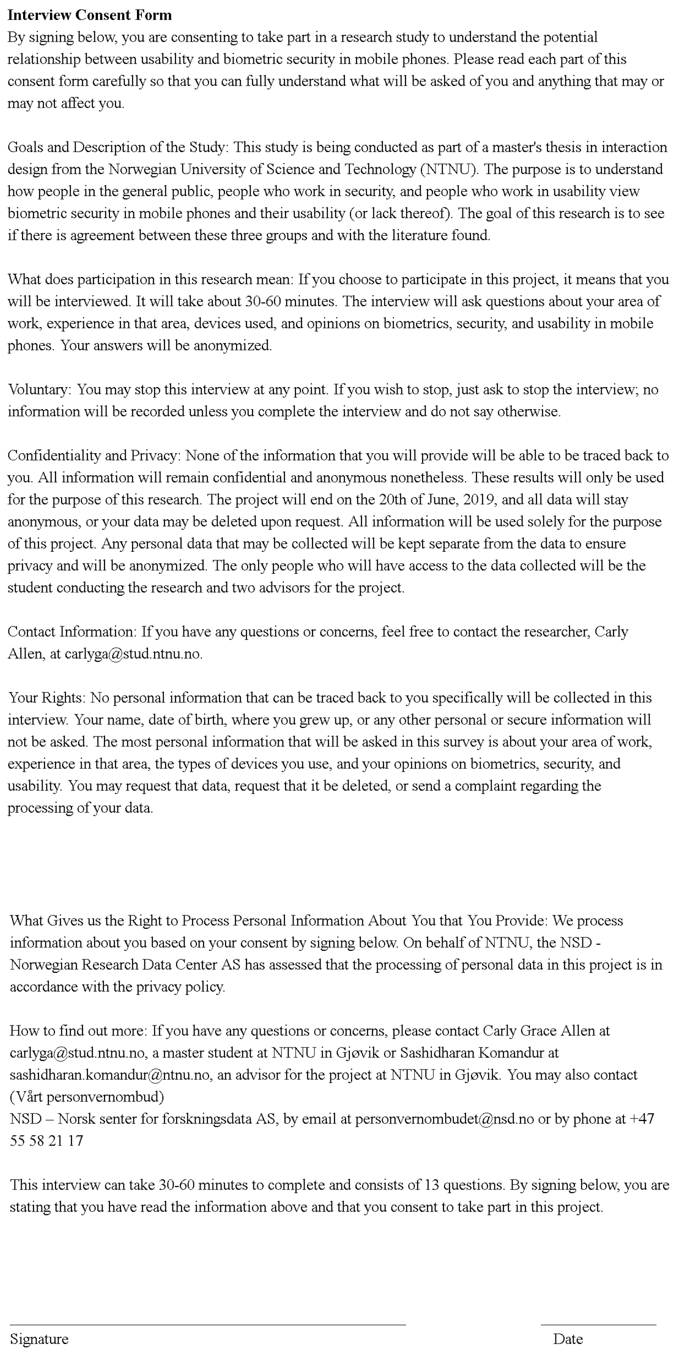
○ A phone that is easy to use is less secure, and a phone that is more secure is not as easy to use
○ A phone can be both easy to unlock and secure (but they aren't always like this right now)
○ Phones are both easy to unlock and secure
○ I mainly care about how easy a phone is to use
○ I mainly care about if a phone is secure to use

Skip to question 38.

Other Thoughts

38. **Do you have any other thoughts or comments about the security / biometric security of mobile or smartphones, or about unlocking your phone overall (how easy or difficult it is)?**

A.4 Interview consent form



Interview Consent Form
By signing below, you are consenting to take part in a research study to understand the potential relationship between usability and biometric security in mobile phones. Please read each part of this consent form carefully so that you can fully understand what will be asked of you and anything that may or may not affect you.

Goals and Description of the Study: This study is being conducted as part of a master's thesis in interaction design from the Norwegian University of Science and Technology (NTNU). The purpose is to understand how people in the general public, people who work in security, and people who work in usability view biometric security in mobile phones and their usability (or lack thereof). The goal of this research is to see if there is agreement between these three groups and with the literature found.

What does participation in this research mean: If you choose to participate in this project, it means that you will be interviewed. It will take about 30-60 minutes. The interview will ask questions about your area of work, experience in that area, devices used, and opinions on biometrics, security, and usability in mobile phones. Your answers will be anonymized.

Voluntary: You may stop this interview at any point. If you wish to stop, just ask to stop the interview; no information will be recorded unless you complete the interview and do not say otherwise.

Confidentiality and Privacy: None of the information that you will provide will be able to be traced back to you. All information will remain confidential and anonymous nonetheless. These results will only be used for the purpose of this research. The project will end on the 20th of June, 2019, and all data will stay anonymous, or your data may be deleted upon request. All information will be used solely for the purpose of this project. Any personal data that may be collected will be kept separate from the data to ensure privacy and will be anonymized. The only people who will have access to the data collected will be the student conducting the research and two advisors for the project.

Contact Information: If you have any questions or concerns, feel free to contact the researcher, Carly Allen, at carlyga@stud.ntnu.no.

Your Rights: No personal information that can be traced back to you specifically will be collected in this interview. Your name, date of birth, where you grew up, or any other personal or secure information will not be asked. The most personal information that will be asked in this survey is about your area of work, experience in that area, the types of devices you use, and your opinions on biometrics, security, and usability. You may request that data, request that it be deleted, or send a complaint regarding the processing of your data.

What Gives us the Right to Process Personal Information About You that You Provide: We process information about you based on your consent by signing below. On behalf of NTNU, the NSD - Norwegian Research Data Center AS has assessed that the processing of personal data in this project is in accordance with the privacy policy.

How to find out more: If you have any questions or concerns, please contact Carly Grace Allen at carlyga@stud.ntnu.no, a master student at NTNU in Gjøvik or Sashidharan Komandur at sashidharan.komandur@ntnu.no, an advisor for the project at NTNU in Gjøvik. You may also contact (Vårt personvernombud)
NSD – Norsk senter for forskningsdata AS, by email at personvernombudet@nsd.no or by phone at +47 55 58 21 17

This interview can take 30-60 minutes to complete and consists of 13 questions. By signing below, you are stating that you have read the information above and that you consent to take part in this project.

_____________________________________ ____________
Signature Date

A.5 Interview guide

Opening Questions

1. What is your job?
2. How long have you been working as a _______? (Based on answer from first question)
3. What devices do you use?
4. What authentication method(s) do you use to unlock your phones?

Discussion

1. What do you think about security for unlocking mobile phones?
2. What do you think about biometric authentication for unlocking mobile phones?
3. Do you think that usability is important/not important when it comes to unlocking mobile phones?
4. Do you think that biometrics are a usable or not usable option for unlocking mobile phones?
5. Do you think that there is a trade-off between security and usability?
   a. If so, why?
   b. If not, why?
6. Do you think we can have mobile phones that are both secure and usable?

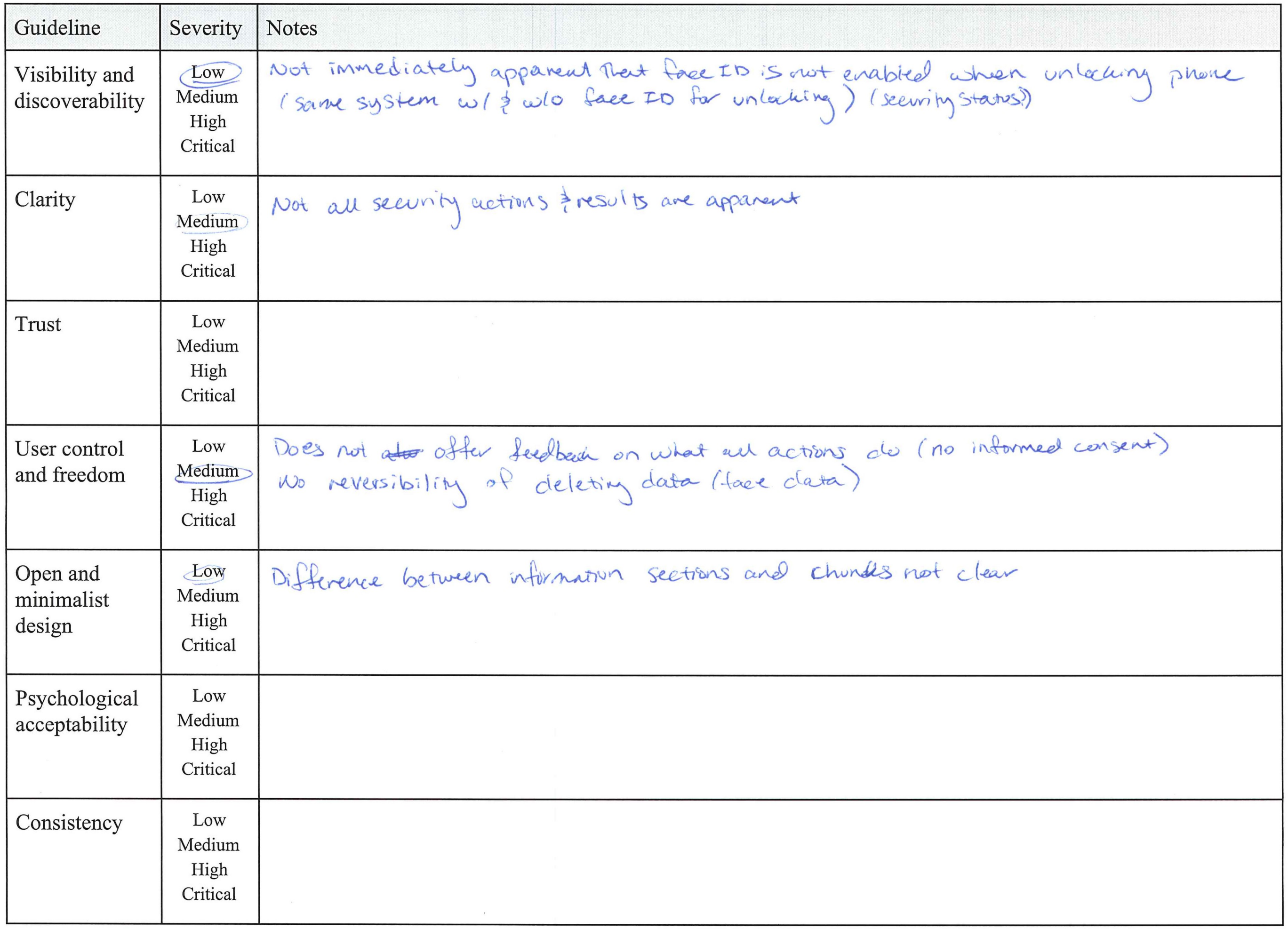
Closing Questions

1. How do you think we could improve both usability and biometric authentication (or security overall) in mobile phones?

A.6 Evaluations

Two of the six evaluation form results are shown here.

Mobile Phone #1 (P1)



Guideline	Severity	Notes
Visibility and discoverability	[✓ Low] Medium High Critical	Not immediately apparent that face ID is not enabled when unlocking phone (same system w/ & w/o face ID for unlocking) (security status)
Clarity	Low [✓ Medium] High Critical	Not all security actions & results are apparent
Trust	Low Medium High Critical	
User control and freedom	Low [✓ Medium] High Critical	Does not ~~also~~ offer feedback on what all actions do (no informed consent) No reversibility of deleting data (face data)
Open and minimalist design	[✓ Low] Medium High Critical	Difference between information sections and chunks not clear
Psychological acceptability	Low Medium High Critical	
Consistency	Low Medium High Critical	

Guideline	Severity	Notes
Feedback	Low [✓ Medium] High Critical	No tactile feedback during set up No feedback or verification before deleting a face IDs
Errors and Help	Low [✓ Medium] High Critical	No help option specific for authentication cannot delete only one face, must delete both if one is to be removed
Effectiveness and constraints	[✓ Low] Medium High Critical	user must swipe after unlocking
Efficiency	[✓ Low] [✓ Medium] High Critical	Once face ID is accepted, the user must swipe open the phone After locking phone, must move it away from the face for the device to re-detect, must swipe from the absolute bottom of the screen
Learnability	Low [✓ Medium] ~~[✓ High]~~ Critical	No introduction to face ID
Defense in depth	Low Medium High Critical	Cannot determine
Authority and privilege	Low [✓ Medium] High Critical	Not clear if revoked privilege also removes data Not clear if amount of privilege changes

Guideline	Severity	Notes
Privacy	[✓ Low] Medium High Critical	No privacy logs? Cannot partially consent; all or nothing
Mappings	[✓ Low] Medium High Critical	Must go to specific location (3 steps) to find privacy information on each option That can use face ID
Security and authentication	[✓ Low] Medium High Critical	Option to require eye contact or not due to sunglasses No desription of how data can be used
Flexibility, customizability , and accessibility	Low [✓ Medium] High Critical	Only one biometric trait available
Isolation	Low Medium High Critical	Cannot determine

Mobile Phone #2 (P2)

Guideline	Severity	Notes
Visibility and discoverability	Low Medium High Critical	
Clarity	Low [✓ Medium] High Critical	Preferences set op not initially clear Not clear why ~~one~~ face or iris stops working Not clear on deleting data it accessed by wrong personmultiple times
Trust	Low [✓ Medium] High Critical	Reduced disklosure on biometriss & data usage
User control and freedom	Low [✓ Medium] High Critical	~~Cannot recover~~ Not clear explicit consent
Open and minimalist design	Low Medium High Critical	
Psychological acceptability	Low Medium High Critical	
Consistency	Low Medium High Critical	

Guideline	Severity	Notes
Feedback	[✓ Low] Medium High Critical	Reduced feedback on when face or iris is accepted for verification Not clear feedback that iris was not accepted
Errors and Help	~~Low~~ [✓ Medium] High Critical	No help for setting up biometric traits
Effectiveness and constraints	Low [✓ Medium] High Critical	must turn on screen to use iris recognition Defaults to faster but less secure face recognition Not clear on where to pick which biometric trait to use as primary option ~~Not feed clear feedback that fac iris is not accepted~~
Efficiency	[✓ Low] Medium High Critical	Defaults to users having to swipe to finish unlocking with face ID, but not with intelligence scan Does not work with sunglasses (face)
Learnability	Low [✓ Medium] High Critical	No introduction to finger print Biometric preferences set up not initially clear
Defense in depth	Low Medium High Critical	Cannot determine
Authority and privilege	[✓ Low] Medium High Critical	Two locations to delete face and iris data

Guideline	Severity	Notes
Privacy	Low [✓ Medium] High Critical	No explicit statement of data use or purpose Privacy logs?
Mappings	[✓ Low] Medium High Critical	Mappings do not always match the user mental model
Security and authentication	Low Medium [✓ High] Critical	No verification of fingerprint No information on where data is stored No warnings of where else the biometric data can be used
Flexibility, customizability, and accessibility	[✓ Low] Medium High Critical	No tactile feedback of a fingerprint verification or sound only one set of irises can be used on a device
Isolation	Low Medium High Critical	Cannot determine

Carly Grace Allen

NTNU
Norwegian University of
Science and Technology