

UNIVERSITY OF OSLO
Department of informatics

**The First Meeting:
Authentication on
Touch Phones**

Master thesis
60 credits

Siri Bergmann Stølen

4. May 2012



Abstract

It has been estimated that the number of mobile users will pass the number of desktop internet users by 2014. The touch phone has become a central part of the ecology of devices and can no longer be overlooked, and the login process is also an important part of this ecology and a precondition to be able to connect to services within the ecology.

The primary objective of this thesis have been to contribute with research about authentication on touch phones, by addressing the challenges to current authentication mechanisms, users mental model of security, eye tracking of authentication mechanisms and accessibility. Throughout the thesis several methods have been applied to get to know users behavior and the their relation to security and authentication mechanisms on touch phones.

It was made a review of several authentication mechanisms, using different types of interaction. The review were based on findings from the interviews showing that the users thinks it is important that these mechanisms are easy to remember and efficient to use. In addition to concepts of direct manipulation, context and recommendations' from W3C. I argue that there all mechanisms have disadvantages, and that context is one of the factors that makes it hard to create usable and secure methods.

The second research question are discussing users mental model of security, and I argue that the technology have been moving faster then the users are able to adapt in terms of security. The research shows that people are not too concerned about security on touch phones. The need for securing the phone is increasing as the content on the phone increases, but the users are not adapting to this, and jeopardize the security for easy and fast access.

Eye tracking were applied to the research to investigate how users interact and look at different authentication mechanisms on touch phones. I argue that there are practical issues and with conducting eye tracking of authentication methods. All authentication IDs are different and comparing them or creating heat maps would therefor not be appropriate. But it is a good method that generates a lot of data that can be used to use to uncover general usability issues.

The final research question is discussing how to approach accessible design of authentication mechanisms, by looking into the concept of universal design and adaptive information systems. I argue that only multimodal user interfaces would be appropriate to add to an authentication process.

The research lead to a lot of findings that about peoples understanding of security and use of touch phones, which can be used in future studies about authentication on touch phones.

Keywords: Touch phones, Authentication, Mental Model, Security, Eye tracking, Accessibility

Acknowledgement

This thesis was written as a part of my master degree in design, use and interaction and the Department of Informatics, University of Oslo. It have been a challenge working with this project, but it has been very interesting and I have learned a lot. Through out the project I have been surrounded with a people that have had an impact on my progress and the end result.

I would like to thank my supervisor Jo Herstad for connecting me with the right people, and his inspiring and motivational feedback. NR and all the participants within the e-Me project for including me, and generously shared their knowledge. I would also like to acknowledge Morten Dahl from Centre for ICT in education for providing me insight of their pilot project Tabia, and Feide for valuable information about their service.

In additional I will thank the informants that have shared their thoughts and experience in probes, interviews and in user testing. I would not have been able to complete the thesis without your contributions.

At the end I would like to thank my fellow students and friends for motivation and support during the final stage of the writing, and for making my master studies eventful and fun. Especially thanks to my housemates Terese Skavhaug and Åshild Aaen Torpe for contributing in making life in Oslo awesome!

Last but not least I would like to show my appreciation to my family for motivating me to higher education and constantly supporting my choices in life.

Siri Bergmann Stølen
May 2012

Table of content

- Abstract II
- Acknowledgement..... IV
- Table of content V
- Figures IX
- Tables X
- 1. Introduction 1
 - 1.1 Motivation 1
 - 1.2 Research questions 3
 - 1.2.1 Research question 1 3
 - 1.2.2 Research question 2..... 4
 - 1.2.3 Research question 3..... 4
 - 1.2.4 Research question 4..... 5
 - 1.3 Delimitations 5
 - 1.4 Chapter overview..... 6
- 2 Theory 8
 - 2.1 HCI 8
 - 2.1.1 User interaction 10
 - 2.1.2 Direct manipulation..... 10
 - 2.1.3 Mental model..... 11
 - 2.1.4 User involvement 12
 - 2.2 Technology 13
 - 2.2.1 Mobile 13
 - 2.2.2 Mobile context..... 14
 - 2.2.3 Web standards..... 15
 - 2.2.4 Framework for authentication and security..... 16

2.2.5	Single Sign-On	18
2.2.6	Screen locks.....	19
2.3	Identity management	23
2.3.1	Login process	23
2.3.2	Biometrics	24
2.3.3	Adaptive information systems.....	24
2.4	Accessibility	26
2.4.1	Cognitive disabilities.....	26
2.4.2	Blind and visually impaired	27
2.4.3	Assistive technologies	28
2.4.4	Universal design.....	28
2.4.5	WAI	29
2.4.6	E-inclusion	30
3	Methods.....	32
3.1	Case study.....	32
3.2	Qualitative research	33
3.3	Ethics	33
3.4	Cultural Probes	34
3.5	Interview	36
3.6	Eye tracking.....	37
4	Case.....	40
4.1	e-Me.....	40
4.1.1	Prototype	41
4.2	The Norwegian Centre for ICT in Education	42
4.3	Feide	42
4.3.1	Tabia	43
4.4	Feide on touch phones	44

4.5	User testing	45
4.6	Students	45
5	Findings	46
5.1	Cultural probes	46
5.1.1	Three questions	46
5.1.2	Photo.....	47
5.1.3	Your mobile	48
5.1.4	Computer and mobile security	48
5.1.5	Notes.....	49
5.1.6	Summary	49
5.2	Interviews	50
5.2.1	Mobile usage	50
5.2.2	Computer Usage	51
5.2.3	Probe responses	53
5.2.4	The cloud.....	53
5.2.5	Probe responses	54
5.3	Eye tracking	58
5.3.1	Feide	58
5.3.2	e-Me	60
6	Discussion	64
6.1	Review of authentication mechanisms on touch phones	64
6.1.1	Risk and security	67
6.1.2	Security and usability	71
6.2	Mental Model of Security.....	72
6.2.1	What is the users mental model of security?.....	72
6.2.2	How can we take advantage of mental models in design?.....	73
6.2.3	Conceptual model.....	76

6.2.4	Mental model diagram	76
6.3	Eye tracking on touch phones and of authentication mechanisms	80
6.3.1	Challenges and problems	80
6.3.2	Interesting findings.....	82
6.3.3	Eye tracking of authentication mechanisms.....	85
6.4	How to create accessible authentication mechanisms?	86
6.4.1	Universal Design and Adaptive Information Systems	86
6.4.2	Multimodal authentication on touch phones	89
7	Conclusion.....	90
7.1	Review of authentication mechanisms on touch phones	90
7.2	Mental model of security	91
7.3	Eye tracking on touch phones and of authentication mechanisms	91
7.4	How to create accessible authentication mechanisms?	92
7.5	Further work	93
8	References	95
	Appendix A	101
	Appendix B	102
	Appendix C	103
	Appendix D	106
	Appendix E.....	107
	Appendix F.....	111
	Appendix G.....	113
	Appendix H.....	114

Figures

- Figure 1.1 Mobile Users > Desktop Internet Users by 2012..... 1
- Figure 1.2 The Ecology of Devices..... 2
- Figure 2.1 Dilbert by Scott Adams (2010-12-17) 8
- Figure 2.2 The Development of Mobile Phones 13
- Figure 2.3 The Login Process 23
- Figure 3.1 Dilbert by Scott Adams (1995-11-08)..... 32
- Figure 3.2 Tobii Eye Tracking..... 37
- Figure 4.1 Dilbert by Scott Adams (2005-08-02) 40
- Figure 4.2 e-Me prototype..... 42
- Figure 4.3 Feide login connected to Inpera attribute storage 43
- Figure 5.1 Dilbert by Scott Adams (2009-03-10) 46
- Figure 5.2 The Mobile Context..... 47
- Figure 5.3 Security and Screen Locks..... 48
- Figure 5.4 Password authentication 48
- Figure 5.5 Password vs. Pattern 56
- Figure 5.6 PIN-code vs. Images 57
- Figure 5.7 Type username and password 59
- Figure 5.8 Chose affiliation..... 59
- Figure 5.9 Read and accept conditions..... 60
- Figure 5.10 Images vs. Pattern 60
- Figure 5.11 Password vs. Pattern 61
- Figure 5.12 Sound vs. Images 61
- Figure 6.1 Dilbert by Scott Adams (2007-11-16)..... 64
- Figure 6.2 The ecology of the touch phone..... 69
- Figure 6.3 green and red terminals..... 70
- Figure 6.4 The relationship between usability and security..... 71
- Figure 6.5 The mental model of a touch phone..... 73
- Figure 6.6 Mental Model Diagram (72) 79
- Figure 6.7 Eye Tracking..... 80
- Figure 6.8 Image vs. Sound authentication..... 83
- Figure 6.9 TV2 Skole – Sign Language..... 87

Figure 6.10 Multimodal authentication 88

Tables

2.1 Risk levels (29)..... 17
2.2 Security Levels (29) 18
2.3 Screen Locks 21
5.1 Mobile habits..... 47
5.2 Evaluation of authentication mechanisms..... 62
6.1 Review of authentication mechanisms 65
6.2 Risk Levels (29) 68

1. Introduction

1.1 Motivation

Mobile phones have always been fascinating to me. I grew up simultaneously as the mobile phone evolved, well you can say that the mobile technology grew faster than me. Even though I was only a child, I can remember the large mobile phones where the handset was connected to a wire, and that you had to carry around in a shoulder bag. The development since that has passed all expectations, if someone had told me that we in just a couple of years would use our phones to play scrabble with friends in other countries, I would never had believed it! This makes me realize that there probably still is lot of undiscovered possibilities when it comes to mobile technology.

As many other people I am registered on a lot of accounts online. I created my first mail account when I went to primary school, without knowing exactly what it was or how to use it. My knowledge of internet and technology in general evolved as I grew up, and especially after I started the University. The changes within the world of technology is moving faster than most of us can keep up with. For only a couple of years ago we could only read text messages and receive images on our phone, but now we also use our phone to look up information on the internet. The trend is changing, as Charles Arthur wrote in The Guardian last summer, the mobile phones are “replacing what we perhaps wrongly thought was an embedded parts of our lives: the PC (1)”. According to the graph in figure 1.1 mobile users will pass desktop internet users by 2014 (2).

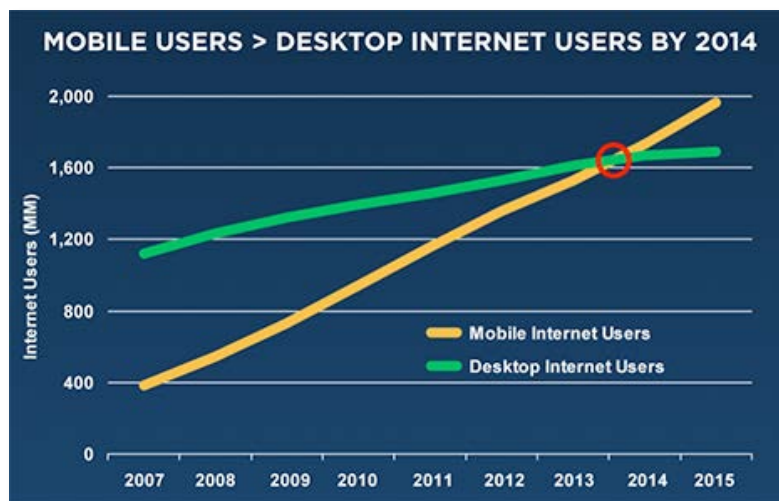


Figure 1.1 Mobile Users > Desktop Internet Users by 2012

We are online all the time and expect to be able to access all kinds of services independent of where we are. According to a report released by comScore, mobile phones generated 10% of the Internet traffic in 2011 (3). This means that we have to understand and design not only for

the PC but also for interaction on mobile terminals. There are several approaches when we design for mobile terminals, we can develop web applications, native applications or hybrid applications. With touch interfaces and small devices, new ways of interaction appear, but we are still in an early exploratory phase. Independent of what solution we choose it is important to always have focus on the users and their relation to the product, according to the tradition of user-centered design.

With new technology new challenges unfold. Among all the challenges security issues have been brought to my attention. Working in a bank have also made me more aware of security and the importance of usability when dealing with technology. With the increased scope and use of mobile phones one would believe that security and authentication on mobile phones would get much more focus then it does today. We are daily using mobile applications like Facebook, flickr, LinkedIn, Dropbox, Skype e.g. which all requires you to login with a user name and password. There are more and more passwords to manage, and remember, and a lot of value at stake. Because of the login process systems with a high level of security are often cumbersome to use which leads to a poor user experience. The amounts of information we keep on our phones have increased significantly, but most of us still only protect our phones with a short pin code. Is this enough? Do we think about the content and context of use when we choose our authentication mechanism? What would happen if a stranger goes access to our mailing and Facebook account? Do we have a correct understanding of what level of security that would be appropriate for our phones?

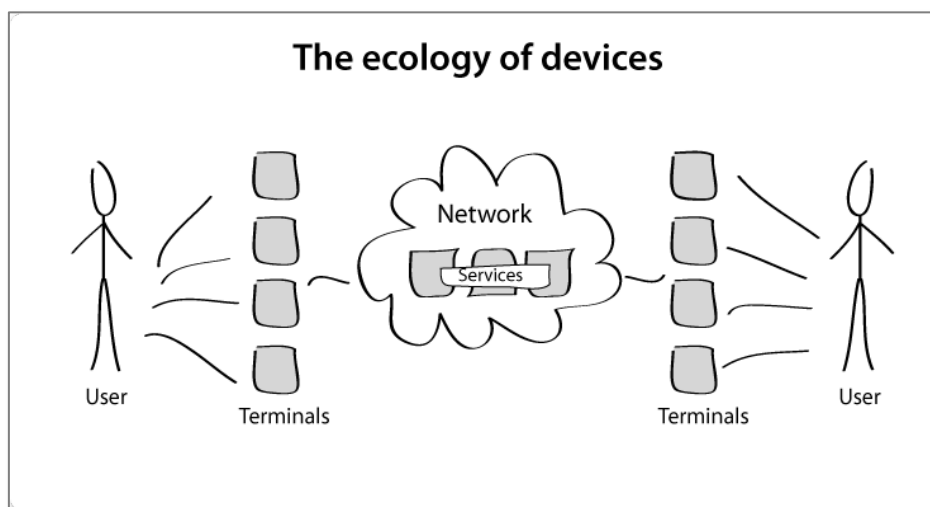


Figure 1.2 The Ecology of Devices

With the rapid development of both the specific technologies and how we talk about technology it is easy to get confused about how everything is connect and interact with each other. As a designer the need to understand the ecology is essential in order to design new technology that will work with the existing ecosystem. Figure 1.2 is an attempt to clarify this. The user is interacting with different terminals, a terminal can for instance be a stationary or mobile device like a phone or tablet, a laptop or a stationary computer. The terminals can be connected to a network, either wireless or with cables and through that communicate with each other, exchange information, content and data (4). The user will have to login to both the

terminals and the networks in order to use them. The reality, and what makes it complicated, is that we are not operating with distinct terminal or device and well-defined boundaries and anymore, but a large set of interconnected terminals connected through different networks (4).

This thesis is written within the field of HCI, and interaction design. Interaction design can be divided into three parts, the understanding of use and practice, design and evaluations. I have been looking partial into concepts of HCI, technology, identity management and accessibility. The research questions are rooted in theoretical concepts like the users mental model, direct manipulation, adaptive information systems.

1.2 Research questions

This is a master thesis in the field design, use and interaction where human computer interaction (HCI) have formed the basis for this project. The main focus was authentication on touch phones, and the thesis primarily addresses issues and challenges related to this. As mentioned it is difficult to draw distinct boundaries within the ecology of devices, and working with authentication it is necessary to include all the different parts of the ecology; users, terminals, and networks in order to get a complete picture. Using four research questions I will examine and go in depth of this and try to come up with research that can bring something new to the field within authentication on touch phones.

1.2.1 Research question 1



Make a review of authentication mechanisms on touch phones.

Mobile phones are not just phones anymore, our phones have turned into small mobile computer terminals containing a lot of information about us and our life. We think it is worse to lose a phone than our wallet, in spite of this the way we access our phones have not changed, most people only use a four digit pin-code and many no code at all. I will investigate different authentication mechanisms and screen locks to get an overview over available options and make a review of them in terms of usability, direct manipulation and context as these are some of the main concepts that separate authentication on touch phones from stationary terminals with GIMP interface.

1.2.2 Research question 2



Examine the term mental model of security. How can we utilize the concept of mental models in design of authentication mechanisms for touch phones?

People's mental models affect how they experience a system and are a condition for understanding it inside their heads. In order to be able to design good authentication mechanisms knowing the users mental model of security is essential.

In general the design of security systems must follow the principle of psychological acceptability: It is essential that the human interface is designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly. Also, to the extent that the user's mental image of his protection goals matches the mechanisms he must use, mistakes will be minimized. If people must translate their images of their protection needs into a radically different specification language, they will make errors (5,6). Answering this question will give more knowledge of the term mental model and information of how authentication mechanisms can be adapted to people's mental model of security?

1.2.3 Research question 3



How can eye tracking and eye tracking software be used as a tool to investigate authentication mechanisms on touch phones?

As a designer or a developer of a web page, you know how you and other people in the design team see the site. You can through observing the users track what links the users click on and how they use the page, but you will not get data on how the users actually look at the page. Eye tracking have been used to learn about how users look at web sites and how that impact what they do on the site. It is simply following the trail of where a person is looking (7), and communicates this data directly to the researcher or observer.

The web are experiencing an increased traffic from mobile devices, and the size and format of the mobile screen might change the way users look at the content. Technology does now also allow us to do eye tracking on mobile devices, and gives us an opportunity to learn more about the users viewing patterns and behavior on this platform, but also to learn about the challenges that eye tracking on mobile devices offers.

Using eye tracking software from Tobii I will investigate user how users look at different authentication mechanisms on their touch phones and analyze the result to see if there are any results that stands out. The login process consists of several steps, and is depending on input from the user. The eye-tracker will tell us how the human eye interacts with the mobile screen during different authentication mechanisms.

In the discussion I will look at challenges and problems that are present when conducting eye tracking on touch phones, but also present and discuss what interesting findings that can be generated from eye tracking on touch phones. In addition the experience with eye tracking of authentication mechanisms and what particular challenges this offers will be presented briefly.

1.2.4 Research question 4



In what way can we create accessible authentication mechanisms on touch phones?

It is becoming important for us to be able to do almost the exact same things on our touch phone, as we can on our stationary computer. This includes being able to log into all of our online accounts as well. If the trend continues like it is today, the mobile internet usage is expected to take over desktop internet usage by 2014 (8,9). We have to take into consideration that the touch phones are different from stationary computers, both the in size, how one interact with them and where they are used. We want to perform the same tasks, but we have to realize that we are using a different tool and have to adapt our design and way of interacting to this in order to create a good user experience.

More and more services are relying on the user to have internet access, and “everyone” will soon access internet with their phones. People that are not able to do this, could end up feeling left out of the society. That is only one of several reason why it is important to make sure to include everyone when designing for the mobile web. The definition of the mobile web will be described later in the theory chapter.

All users are different and have different preferences. The two types of disabilities that will be mentioned in this thesis is blind and visually impaired users and people with cognitive disabilities. Websites and services in general and how these can be made accessible have been addressed by for instance W3C (10,11). Fuglerud and Dale (12) have found that current authentication mechanisms pose many barriers to various user groups, and that it has to this date been done relatively little research on inclusive authentication mechanisms. It is no point for a web page or service to be accessible if the user is not able to log in.

There are several different approaches when designing accessibility solutions. Within the area of universal design and identity management systems we find three types of adaptive information systems, multimodal interfaces, user-controlled identity management systems and profiling. These approaches will be discussed and I will explore how they can be applied to a mobile touch interface in order to create accessible authentication.

1.3 Delimitations

The main focus in this thesis have been on authentication on mobile phones, limited to touch phones. The emphasis has been on analyzing how people relate to security on mobile phones, compared to the security on computers.

Feide login is used as a case to prove insight into the issue. Feide is a technology that is used by both students and employees on about 44 services at the University of Oslo. I have chosen to limit this thesis to focus on students and the services available for them. Several factors had an impact on this decision, both my own interest as a user of Feide login and good access to test users and informants was important.

I have looked at the login process with emphasis on the authentication in the login process. While the creation of user accounts and authorization is outside the scope and will only be mentioned briefly and not discussed on this thesis.

Based on the data that was collected during this study I have chosen to focus mostly on how users of touch phones relate to and understand security on touch phones, how this affect their usage patterns when it comes to authentication, and how this knowledge could help to improve design of authentication mechanisms.

From an academic perspective, I have discussed the key principle within interaction design literature, as well as more specialized topics as universal design adoptive information systems and mobile context, in addition to methods for data collection. Since most application on touch phones are only logged into once, the screen lock is often the only security protection activated and will therefore be central in this paper.

It has been done research in how eye tracking can be used as an input technique for assistive technology. For people that cannot use their hands and arms using their eyes can be a solution. Nielsen (7) states that eye tracking can be a great tool for disabled uses "because it allows them to point to objects on the screen and activate them with just a blink of an eye". However in this project the focus will only be on eye tracking as a tool to test the user interface in an evaluation phase.

1.4 Chapter overview

The structure of this paper reads as follows:

Chapter two, theory, explains concepts that will be relevant through out the thesis. It is divided into four parts; HCI, technology, identity management and accessibility.

Chapter three, the method chapter all of the qualitative methods used to gather data will be described together with details of how the research were conducted. This includes cultural probes, interviews and eye-tracking.

In chapter four the case, including all parties involved in this thesis are described. This includes among others the users, the research group e-Me, The Norwegian Centre for ICT in Education and Feide.

After the methods and the practical details the findings from the cultural probes, interviews and eye tracking are presented. These generated a lot of data, which has been documented with pictures and quotes in the fifth chapter.

Several methods have been applied in order to increase the reliability of this study. The methods complement each other and are intended to enable the research questions to be answered in the best possible way. In chapter number six the findings from the different methods will be discussed with the theoretical aspects that have been described earlier as a basis.

The thesis ends with a conclusion based on the discussion together with thoughts for further work within this research field.

The appendixes can be found on page 106. These includes information about Feide, a copy of the probes that were used and consent forms for the interviews and eye tracking. In addition the interview guides, the password security meters that were tested and gaze plots extracted from the eye tracking data.

2 Theory

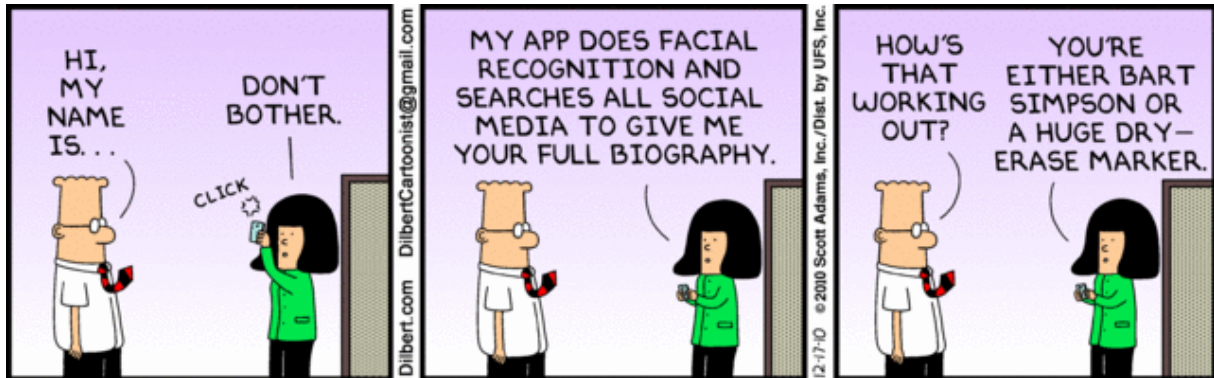


Figure 2.1 Dilbert by Scott Adams (2010-12-17)

In this chapter I will describe the main concepts and terms that will be discussed later in the thesis. This involves an explanation of the general terms like human-computer interaction and usability as well as the mobile context and accessibility.

2.1 HCI

HCI or human computer interaction is forming the framework of this paper. The direct understanding of this term is the interaction between a human and a computer. Sharp, Rogers and Preece (13) explains that:

“HCI has traditionally involved the design, evaluation, and implementation of interactive computing systems for human use and with the study of major phenomena surrounding them (13).”

The term computer is no longer limited to what we know as a computer with a keyboard, a large screen and a hard drive. When we talk about HCI we are also including interaction with other devices like tablets, phones, automatic ticket machines, GPS, the display on a microwave and so on.

A central concept in HCI is usability. There exists numerous definitions of the term usability. Sharp, Rogers and Preece (13) explains that usable products should be easy to learn, effective to use, and enjoyable from the users perspective. While the International Organization for Standardization (ISO) defines usability as “the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use”. Usability does not only relates to understand what a particular action means in the context of a particular interaction, but also to whether the user understands the implications of his or her choices in a broader context (14).

These definition can seem a bit too abstract, but according to Steve Krug (15) usability just means that something works well: that a person of average (or even below average) ability

and experience can use the product – whether it's a Web site, a fighter jet, or just a revolving door – for its intended purpose without getting hopelessly frustrated.

In order to achieve usability in a product Krug suggests that you follow three laws (15).

1. **Don't make me think** is Steve Krug's first law of usability. By this he means that a web page should be self-evident, obvious and self-explanatory as far as it is humanly possible.
2. The second law reads: **It doesn't matter how many times I have to click, as long as each click is a mindless, unambiguous choice.** This refers to the first law, and is quite self-exploratory. Some states that there should be no more than three click for the user to achieve the desired goals. However Krug States that as long as the navigation is easy and logical for the user the number of clicks is irrelevant.
3. **Get rid of half the words on each page. Then get rid of half of what's left.** Web pages are often filled up with needless words in form of instructions and welcoming messages that no one reads. By removing them, the level of noise on the page is reduced, the most important content get more attention and it makes the page shorter and then easier to get an overview over the content without having to scroll.

Nielsen have created a set of ten heuristics that one should have in mind when designing for user interface (16,17), these goes more into details and elaborates Krugs laws.

The first three heuristics is about visibility, conventions and user control and freedom. The system should keep the user informed of its status by providing appropriate feedback. To make sure that the users understand the system one should follow real-world conventions and stick to familiar words, phrases and concepts. Even when following these guidelines users will often choose functions by a mistake, which makes it important to add clearly marked exits and support undo and redo.

In addition to following real-world conventions Nielsen stresses the importance of following the platform conventions, and be consistent in the wording to avoid creating confusion for the users. Understandable help and documentation should be provided when needed, however “even better than a good error message is a careful design which prevents a problem from occurring in the first place.” This can be done by for instance make the user confirm its actions.

As Krug mentions in his first law, don't make me think, this is also what Nielsen express when embracing recognition rather than recall. By making objects, actions and options visible the user's memory load is minimized. The users of a system might have different experience, but by adding so called accelerators or shortcuts for expert users a system can cater both inexperienced and experienced users.

Krug states that webpages often are filled up with unnecessary words, and that by removing them would make them more user friendly. Nielsen has come to the same conclusions that irrelevant or rarely needed information is fighting for the attention of what's really important, and should therefor not be included.

Both Krugs laws and Niensens heuristics are general guidelines that can be apply to all types of systems on all kinds of devices independent of what type of user interaction it they use.

2.1.1 User interaction

There are multiple types of user interfaces that can be used to design for user experience (13). Some focus on the function of the interface, like to be intelligent, to be adaptive or to be ambient, while others focus more on how the interaction works, command, graphical, pen-based, and speech-based or what platform it is designed for, like PC or mobile. In the 1980's the acronym WIMP, now called GUI (graphical user interface) was introduced as an alternative to the command-based interface. This was a new way of represent the core features of an interface for a single user. The information was now presented with windows, icons, menus and pointing devices that could be manipulated by the user. This was the first meeting with direct manipulation and the desktop metaphor.

2.1.2 Direct manipulation

Ben Shneiderman described in 1983 direct manipulation as the ability to manipulate digital objects on a screen without the use of command-line commands(18). He was then referring to input devices like the mice and the joystick and the introduction of the desktop metaphor. With touch screens and gestural interfaces direct manipulation got a new meaning. We are now talking about using the body to directly manipulate and control the digital space, with scrolling moving, zooming and so on (18). Sharp, Rogers and Preece (13), describe direct manipulation as a form of interaction that involves manipulating objects based on the users' knowledge of how they do so in the physical world.

There are many reasons to use a gestural interface. Natural interaction is one of them, interacting directly with digital objects in a physical way make the interaction similar to how it would be in a natural environment. Another advantage is that there are less need of hardware because accessories like the mouse and keyboard is removed. This makes it more flexible, as there are lots of places where it is impractical or out of place to use a traditional computer. For instance in stores, museums, airports, and other public places. It is however not just the reduction of hardware that makes gestural interfaces flexible. Touch screens allow for many different configurations, buttons are not fixed and can be changed based on the requirements of the system (18).

While a mouse, a track pad and a keyboard only have a certain number of features and functions, using the body to control a digital interface gives almost unlimited number of ways to interact and there are still a lot more to explore. The new way of interaction is providing a more hands-on experience which encourage to play and exploration of the system (18). The game consoles Wii and Kinect are examples of this.

In spite of all these advantages gestural interfaces is not always the best solution. Saffer also mentions several reasons why a gestural interface might not be a good option.

If there are a need for heavy data input, a system is depending on large amounts of text or number input from the user a physical keyboard is decidedly faster than a touchscreen keyboard for most people to use. The broader and more physical the gestures are the more demanding are they. Age, infirmity or environmental conditions can make it hard for people to perform such gestures. As for environmental conditions, cold weather can be crucial because using a touch screen with gloves on is very difficult. Smaller and more subtle movements can also create problems. The keyboard on a touch screen clearly demonstrates this, because of the small keys people with larger fingers will have difficulties typing.(18)

On most touchscreens there is little or no haptic affordance or feedback when an action has taken place, such as when a button is being pressed. In general touch screens often rely entirely on visual feedback and might therefore create a bigger challenge for visually impaired users.

When designing gestural interfaces it is important to have the context in mind, so that the gestures work in the intended environment. If not, gestures can affect the privacy or may cause embarrassment. On mobile devices it can be difficult to predict the context of use which is one of the reasons why designing for mobile can be a challenge. Gestures can often be visible by others; this is also the reason why they often are used on social systems (18). Using gestures in public for authentication can affect the privacy. Large buttons on a touch device can reveal sensitive information, which the user do not want to expose in public. For instance PINs, passwords, names, credit card information or addresses(18).

2.1.3 Mental model

According to Susan Carey(19) users' mental models come from their prior experience with similar software or devices, assumptions they have, things they've heard others say, and also from their direct experience with the product or device.

Many aspects of human-interaction with computers involve complex processes, and when interaction with computer systems some type of mental model of the process is a precondition (20). In the Handbook of Human-Computer Interaction (20) the difference between mental models and user models are described like this; the expectations users have of a computer's behavior or what they should do with it comes from mental models while the "expectations" a computer has of a user come from user models. In other words it is considered to be the way in which people model processes (20).

Because mental models only are in the user's head and is not directly observable, it is helpful to have models of mental models in order to discuss them. These models are called conceptual models (20). Users conceptual model is a model that represents what the user is likely to think, and how the user is likely to respond (21). Conceptual models can be created through predictions, explanations and diagnosis, training and other evidence like reaction times for eye movements and answering questions about the process (20). Metaphors like desk, folder etc. is the key elements of a user's conceptual model.

Peoples mental model varies, a normal user would probably have a simpler mental model of the system compared to the system administrator. However, Helander, Landauer and Prabhu (20) states that training based on conceptual models about processes can lead to improved performance on tasks requiring an understanding of those processes. Users of computer applications have mental models of the effect of commands in operating these applications. This can for instance be, when typing inn a password and a user name the user expect to enter the application after clicking 'login'. Or a product key, are expected to unlock and give the user access to a software.

Mental models are also subject to change, but selection of appropriate text and graphics can aid the development of mental models. For instance can important features in an app be highlighted, things that belongs together should be placed together or have a similar look to emphasize their relation to a particular concept.

A challenge with creating conceptual models from mental models is that they may be incomplete and can also be internally inconsistent. Often people apply their knowledge and experience from one task to another; however this transfer can create a conflict if the task proves to be different.

Conceptual models reflect that mental models are not directly under our control. In order for the users to acquire the 'right' mental model there are mainly three measures to include, training, documentation and guides or online help and last interaction with the system(22). As documentation and guidelines are read by very few, interaction is usually the only realistic approach (22). In order to create systems that are easy to use based on a conceptual model it requires it to be simple enough to understand only through interaction, deliberately designed and adapted to the users' tasks. One should use familiar concepts and terms, provide adequate feedback and be consistent (22).

Because of the variations in peoples mental models it is important to include and get to know the target group of the product.

2.1.4 User involvement

When working with HCI design user involvement is essential in order to design products that people actually can and will use. User involvement means including people that are affected by the decisions, or are users of the service, and let them influence the decisions and design related to the system or service (23). In this thesis this means students that use the service Feide. The purpose of this is that the developers should learn from the users. User involvement is about taking advantage of users to make appropriate choices when it comes to technology. According to Halback et. al (23) this will contribute to the development of inclusive ICT and provide user-friendly systems and services.

Users with special needs are very important partners to include. When users with impaired functions, like blind or users with cognitive challenges, participate in system development, the will contribute to inclusive design of system or services. Halback et. al have defined

several effects with the increased availability that comes from inclusive design (23).

- The user mass increases (citizens, customers, employees).
- The user will find and solve the problem themselves.
- There will be less pressure on customer services and support
- Development and maintenance can be less expensive: the use of accessibility standards simplifies the development process, and this can lead to less need for basic testing.
- Starting out with accessibility on an early stage saves resources compared to having to adapt afterwards.

It is an advantage to involve disabled early in the process as it is high probability of revealing accessibility issues even if there are only a small number of participants (12). In other words user involvement promotes usability and increases the accessibility, and accessibility is profitable.

2.2 Technology

2.2.1 Mobile

As this project is evolving around mobile phones it is natural to take a look at where we are today in terms of mobile use. The last few years' numbers of touch phones have increased dramatically, and there is no reason to believe that this development will stop. Mobile phones in general play a central role in our everyday life, and for only a couple of years ago we had never heard of touch phones or phone applications, and now we use them all the time and can hardly live without it.

There are large differences on what type of phones that are most used in the different part of the world. While feature phones are still dominating the markets in developing countries it is the touch phones that dominates the market in the western world. To clarify what type of mobile phones this thesis is dealing with, the following section will describe three different phone categories; feature phones, smart phones and the touch phones, and how they technology have evolved. These three types of phones overlap and there are still people using both feature phones and smart phones today.

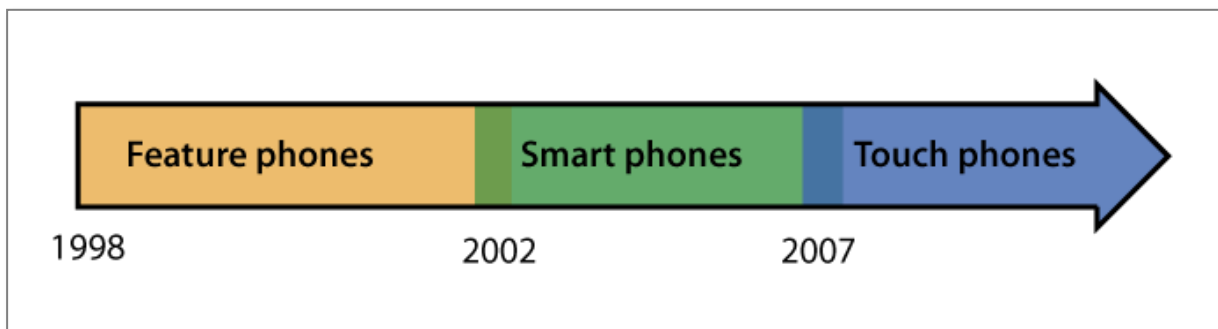


Figure 2.2 The Development of Mobile Phones

Before feature phones were introduced in 1998 mobile phones could only do three things, make voice calls, send text messages and play snake. The feature phones now also gave us the opportunity to play around with various applications and services, like listening to music and take photos (16). The web had also reached the mobile device, but because of high prices, poor marketing and inconsistent rendering almost no one used it. Instead of improving the web the mobile companies focused on selling ringtones, wallpapers, games and applications through network operator portals (16).

In 2002 the first smart phones appeared, by learning from desktop computing mobile phones strived to become personal computers. Fling (16) states that the reason smart phones have never really been defined is it's similarity to feature phones. Smart phones have a lot of the same capabilities as feature phones do, making phone calls, sending SMS, taking pictures and accessing the web. But in addition to this most smart phones came with an common operating system, a larger screen and a QWERTY keyboard or stylus for input, and Wi-Fi or another form of high-speed wireless connectivity (16).

Dominated by the iPhone the touch phones era introduced a completely new media that offered new ways of interact and understand information (16). Instead of using a key pad the interaction were now moved to the large touch screen. Another new feature was that the touch phones also leverage location and movement.

This thesis will mostly refer to touch phones, but common for all phones is that they, different from stationary devices, are with us everywhere and used in a lot of different contexts.

2.2.2 Mobile context

The desktop context involves information that we access typically stationary while sitting at our desk. The mobile web however including sites and web applications designed for mobile devices, or the mobile context, which we can access anywhere at anytime. Whether there is something that should be called the mobile web or not have been discussed, but Brian Fling (16) states that the terms of the technology that we use to publish information and knowledge is the same, it's just a difference of how and where it is presented.

Fling divides mobile context into context with a capital C and context with a lowercase c. He describes Context as how the users will derive value from something they are currently doing. In other words the mental model the users will establish to form understanding. He states that “the context enables us to better understand a person, a place, a thing, a situation, or even an idea by adding information to it (16).”

What Fling refers to as context with a lowercase c is the more common understanding of the word. It is “the medium, mode, or environment in which we perform a task or the circumstances of understanding (16).”

This thesis will touch upon how peoples understanding of a context affect how a task is performed, in connection to the mobile authentication case. Donald A. Norman states that better understanding creates better security(24). A known issue is that people creates too easy

and insecure passwords, but by having a clear conceptual model and give the users better feedback it will make it easier for them to understand the requirements for the use of the system. What is especially interesting in this case is if people's mental model changes as we are moving around and how this affects the level of security, and the interaction with the device.

There are a lot of considerations to take when designing for mobile devices. Luckily there have been made guidelines and standards that can make this process easier.

2.2.3 Web standards

Blind and partially sighted is a complex target group, as there are many different factors to consider. A person that has been blind the entire life may experience things different than a person that became blind as a grownup. Similar, a person can be partially sighted in various degrees. These factors make it difficult to find solutions that are suitable for everyone. Assuming that there are similar variations also within other types of disabilities.

This brings us to web standards. It seems impossible to create a design that is perfectly adapted to all kinds of disabilities, but it is possible to create solutions that are suitable for many different people. Web standards are created to ensure that technology are working in the *best* possible way and in the *greatest* possible extent is accessible and user-friendly for everyone; regardless of disability, platforms or devices.

The international community the World Wide Web Consortium (W3C) has for a long time had a vision about "leading the World Wide Web to its full potential by developing protocols and guidelines that ensure the long-term growth of the Web (25)." One of their principles that guide their work is the principle of creating a *Web for All*.

"The social value of the Web is that it enables human communication, commerce, and opportunities to share knowledge. One of W3C's primary goals is to make these benefits available to all people, whatever their hardware, software, network infrastructure, native language, culture, geographical location, or physical or mental ability (25)."

W3C (25) have created a set of guidelines to make web content more accessible (WCAG 2.0) (11), in addition to this they have defined three levels of conformance, A (lowest), AA, and AAA (highest). The different layers are saying something about how accessible the design is, and which requirements that are met, according to WCAG 2.0 (11).

- **Level A:** For Level A conformance (the minimum level of conformance), the Web page satisfies all the Level A Success Criteria, or a conforming alternate version is provided.
- **Level AA:** For Level AA conformance, the Web page satisfies all the Level A and Level AA Success Criteria, or a Level AA conforming alternate version is provided.
- **Level AAA:** For Level AAA conformance, the Web page satisfies all the Level A,

Level AA and Level AAA Success Criteria, or a Level AAA conforming alternate version is provided.

Although these web standards just are recommendations from W3C, they are important for the development of today's technology. WCAG 2.0 is focusing on web technologies and accessibility, but in addition to these guidelines W3C have provided some basic guidelines for Mobile Web Best Practices 1.0 (26). The guidelines are directed towards creators, maintainers and operators of websites and has as main objective to improve the user experience of the Web when accessed from mobile devices (26).

Point 5.5.1 deals with user input on mobile devices, and are referring to mobile devices lack of pointing devices and standard keyboard for text entry (27). W3C recommend that the numbers of keystroke are kept to a minimum and that free text entry should be avoided where possible. To reduce the amount of input pre-selected default values should if possible be provided, and the default text entry mode, language and/or input format should be specified, if the device is known to support it.

WCAG 2.0 and other web standards are essential and are the foundation when new laws are being drafted and proposed.

2.2.4 Framework for authentication and security

The renewal, administration and church ministry have created a framework for authentication and security in electronic communication with and within the public sector (28). The guidelines apply to public entities that facilitate online services and cooperative interaction online. The document contains recommendations for implementation of risk analysis and selection of security level when authentication is needed. They have divided the requirements into two categories, authentication for persons and authentication for organizations and businesses. Only the requirements for persons and what concerns authentication will be mentioned in this section.

Increased electronic cooperation leads to a greater need for coordinating the methods for authentication that are used. According to the published framework (28) common security levels in the public sector will provide the opportunity for reuse of security solutions or the use of common security solutions, communication with users of public electronic services. It recommends this approach as reusing solutions improve usability for the users and leads to savings in public businesses. Common security-levels will also provide increased assurance that interacting government agencies ensure information exchanged in an adequate manner.

Common risk levels is the first step to pave the way for joint solutions and re-use of authentication solutions. The risk is calculated by the probability and consequence, in the mentioned framework there is a table that defines four risk levels. This can function as a facilitator when deciding which risk level to chose.

2 Theory

2.1 Risk levels (29)

	Risk level 1 None	Risk level 2 Small	Risk level 3 Moderat	Risk level 4 Large
Consequences for health and life	There are no danger of loss of life and / or human health.	There can be small injuries	There can be moderate injuries	There may be loss of life and / or public health
Economic loss/ more work/ increased costs.	No economic loss/ more work/ increased costs	It can lead to small economic loss / additional work / increased costs	Violations can result in moderate financial loss / additional work / increased costs	Violations can result in large financial loss / additional work / increased costs
Loss of reputation (reputation, trust and integrity)	No damage to reputation.	Any damage to reputation is considered to be small.	Reputation may be somewhat impaired in a shorter period of time.	Reputation may be impaired for a long time, eventual lasting.
Obstacle in criminal prosecution	No contribution to the prevention of criminal prosecution.	Minimal contribution to the prevention of criminal prosecution.	Moderate contribution to the prevention of criminal prosecution.	There may be obstacles in the prosecution.
Negligent contribution to the offense	It can not be negligent assistance to crime.	It can not be negligent assistance to crime.	It can not be negligent assistance to crime.	Violations may contribute to negligent assistance to crime.
Inconvenience / disadvantages	No nuisance or inconvenience.	There can be some inconvenience or hassle.	Not relevant.	Not relevant.

While risk level 1 is intended for open information. Functions and information exchange in related to confidential or person sensitive information must be at the other levels of risk according to the likely consequences that could occur if the adverse event occurs (29).

Below is exemplified adverse events that may lead to consequences in the table above (29).

- Unauthorized alteration of patient data.
- A person's disease diagnosis becomes known to unauthorized persons.
- Figures leak out before the quarterly reporting.
- Errors in payment of social security foundation.
- Errors in utbetalingsrunnlag for VAT.
- Unauthorized changes to influence public payments.
- Public agencies are losing reputation after media coverage of data breaches.
- Proof material is damaged or go astray, because of operator error.
- Unauthorized modification of personal address as part of identity theft.

The Government is working with four safety parameters (29) when it comes to authentication and security in electronic communication in the public sector. Social media like Facebook and Twitter is not legally required to follow these guidelines, but they can provide guidelines to what level of security they should be placed on. Regjeringen.no defines the security parameters as follows: "A security parameter is a factor that affects the security of the solution

if it changes. An example of such factor is "extradition to the user". For a password solution will "extradition to use" describe how the password in practice is distributed to the user (29)."

The security is defined using four different security parameters: Required authentication factor(s), delivery to the user, security requirements and requirements for public approval. Required authentication factor(s) describes the number of authentication factors and their properties. An authentication factor can be either static or dynamic. Static means that the documentation presented to others to verify the claimed identity, does not change from time to time. An example of this is the fixed password, or biometric data.

The level of security for a service is chosen based on the risk level. There are also defined four security levels, and in table 2.2 there are mentioned examples for what authentication mechanisms that would be appropriate for the different levels

2.2 Security Levels (29)

Security level	Examples
1	<ul style="list-style-type: none"> - Self-defined password and username on the web - Identification with personal security number
2	<ul style="list-style-type: none"> - fixed passwords sent out in letters to address in the national register. - Password calculators without password protection, minimum distributed through address in the national register. - Lists of one-time password distributed to address in the national register.
3	<ul style="list-style-type: none"> - Password calculator protected with a PIN code, where the first PIN code is sent in a separate shipment. - One-time password on the mobile phone, where the mobile phone is registered with a registration code distributed to address in the national register. - Person Standard, according to Specification for PKI in the public sector. - Lists of one-time password used in conjunction with a fixed password and username. Choice of fixed passwords should be based on a one-time code sent to address in the national register (or the first-time password code on the list).
4	<ul style="list-style-type: none"> - Sending a letter code in the user expects to receive, and will inquire for. - Confirmation of the activation of the security solution in a separate letter. - Check the mobile phone against a user register - Limited lifetime of transmitted codes

The public sector are responsible of performing their own risk and vulnerability analysis, but the general recommendations id that with risk level 1 security level 1 should be applied and so on (29).

One mechanism that are used extensively across public service is the Single Sing-On mechanism.

2.2.5 Single Sign-On

Single Sign-On (SSO) is a mechanism that is used in order to simplify the login process. With only going through one single authentication and authorization the single sing-on mechanism permit the user access to all computers and systems where he has access permission. This

saves the user from entering password and username multiple times. The Open Group¹ states that single sign-on reduces human error, which is a major component of system failure and is therefore highly desirable but difficult to implement (30).

There are several benefits with using a single sign-on mechanism (30).

- The time it takes for the user to sign-on is reduced, and as a result of this the possibility that the sign-on operation fails are also reduced.
- The security will be improved as the user doesn't have to handle and remember multiple sets of authentication information.
- Administrating the system, adding and removing users or editing their access rights, will be less time consuming, and more responsive.
- The security will also be improved because the system administrator will have an enhanced ability to maintain the integrity of user account configuration. Which includes the ability to limit or remove, an individual user's access to all system resources in a coordinated and consistent manner.

One single sign-on service is OpenID. OpenID is a simple identification mechanism that was created by Brad Fitzpatrick for LiveJournal. It consists of a distributed, decentralized network, where one's identity is a URL that will be verified by a different server that supports protocol (31).

OpenID is an interesting technology to look into, as it offers use of an existing account to sign in to multiple web portals, without needing to create new accounts (32). With OpenID, your password is only given to your identity provider, and that provider then confirms your identity to the websites you visit. Other than your provider, no website ever sees your password, so you don't need to worry about an unscrupulous or insecure website compromising your identity (32). You can choose the identity provider you want, and there exist many providers or hosts such as Google, Wordpress, flickr, Yahoo! and Facebook. In Norway we also have MinID and BankID which are based on the principles of SSO.

As explained in the introduction there touch phone is only a part of the ecology of devices, and all parts of the ecology can be secured with different login mechanism with different security level. It is not default when buying a new phone, but most mobile phones can be secured with what we call a screen lock.

2.2.6 Screen locks

New opportunities have emerged after the touch phone was introduced, also regarding screen locks and phone locks. Screen locks are exactly what it sounds like, a way to lock the screen, and protecting the terminal from being used. One of the most common screen locks for touch

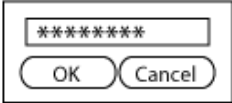

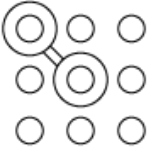
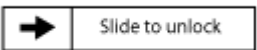
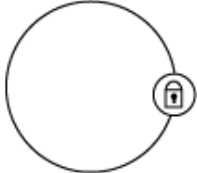

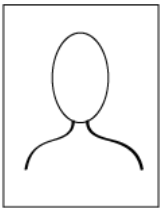
¹

<http://www3.opengroup.org>



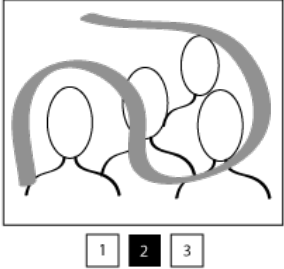


phones is the four digit pin-code, but most android phones does also have password and pattern as options. The new Android 4.0 also called Ice Cream Sandwich does now allow users to unlock their phone with face recognition (33). In addition to the native features there are screen locks available on Google play and Apple Store.

The table under presents several authentication mechanisms and screen locs and describes how they would work on touch phones and stationary terminals ie WIMP interfaces.

2.3 Screen Locks

Method	Feature	Touch phone	WIMP terminals
Password 	Entering a password on the touchscreen.	On screen keyboard is hard to interact with. Special characters makes it more cumbersome as one have to switch between keyboards.	Easy to write with an external keyboard.
Pin-code 			
Pattern 	Dragging the finger on the screen in a predefined pattern.	Touch screen and direct manipulation makes this easy to perform with one finger.	Will not work that well when using a mouse pointer. A large screen makes it easier for unauthorized people to see the pattern.
Slider 			
Circle (Asus) 	Drag the lock inside the circle.	Easy to perform with one finger, but is not secure because everyone can unlock it.	Will not work that well when using a mouse pointer. Is not secure because everyone can unlock it.
Voice recognition 			
Face recognition 	Compare facial features in memory with a face scanner (camera)	The phone needs a user-facing camera with high resolution. Can be easily hacked with a photo.	The terminal needs to be connected to a camera. Can be easily hacked with a photo.

2 Theory

Fingerprint recognition			
	Compare fingerprint pattern in memory with fingerprint scanner.	The screen on touch phones are not sensitive enough to read fingerprints.	The terminal needs a fingerprint scanner.
Piano			
	Play a combination of tones on the piano keys and compare it with predefined tones.	Natural to play a piano with your fingers. Not secure without headphones as unauthorized people can hear the times.	Will not work that well when using a mouse pointer. Not secure without headphones as unauthorized people can hear the times.
Picture gesture			
	Choose a picture, draw 3 gestures, size, position on picture, and direction, as the combination of these attributes will become picture password.	Touch screen and direct manipulation makes this easy to perform with one finger.	Will not work that well when using a mouse pointer. A large screen makes it easier for unauthorized people to see the pattern.
Proximity-based			
	Use a security token that communicate with the mobile using Personal Area Network (PAN) for instance Bluetooth. When the token is in proximity of the mobile the phone is unlocked	The terminal needs to be connected to a PAN network. The are two devices to take care of, and they should not be stored together.	The terminal needs to be connected to a PAN network. The are two devices to take care of, and they should not be stored together.
Near field communication (NFC)			
	Swipe or touch the phone over an NFC/RFID tag to unlock the mobile.	The terminal needs an NFC reader, which is not very common. The are two things to take care of, and that should not be stored together.	The terminal needs an NFC reader, which is not very common. The user must make sure not to loose the NFC-tag.

These screen locks will be reviewed closer later in the discussion. This will be done by comparing the interaction, and investigating the interaction according to accessibility and peoples mental model.

2.3 Identity management

2.3.1 Login process

Independent of what device a system is running on a central part of the system is the login process. The process where a user logs in to a system can be divided into three steps, identification, authentication and authorization (34). All of the three steps will be described, but the main focus in this project have been on the second step in this process, authentication which is what will be most emphasized.

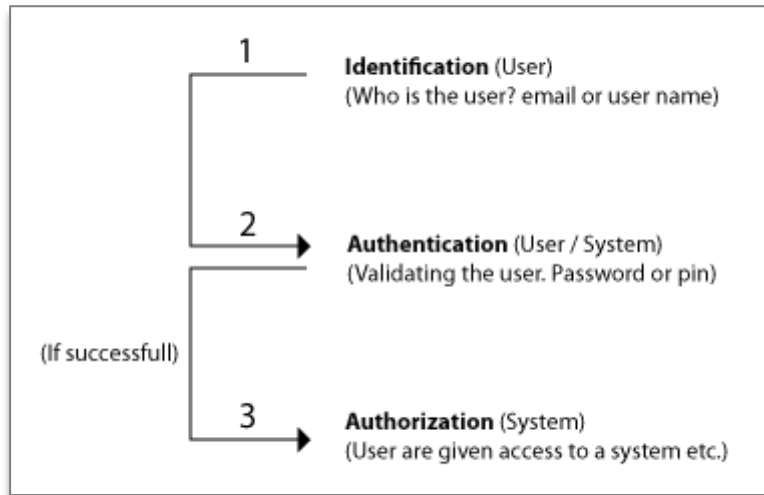


Figure 2.3 The Login Process

Identification is the first step in the login process. Identify means to recognize, determine identity, complete equality between two or more people or things etc. (35). On a webpage the identity is often a user name or an e-mail address. The system uses the input to check whether the user is registered user or not. This can be done as a part of a process or as a single event. A common metaphor is to say your name and show identification for instance a passport.

After identification the user needs to authenticate him self. Authentication is the process of identifying an individual, traditional authentication mechanisms are based on passwords and tokens(36). Electronic authentication often includes magnetic cards, the exchange of electronic keys and PIN codes as well as encryption.

The mechanisms used for authenticate humans are different from the once that are used to authenticate programs and machines. The main reason is because people's capabilities are very different from computers capabilities. Computers can do large calculations quickly and correctly without problems, and have large memories in which they can store and retrieve GB of information, while humans don't (37).

Schneider (37) states that all approaches for human authentication rely on at least one of the following things: Something you know, something you have and something you are.

Something you know, for instance a password, is the most common way to authenticate humans, and they are used to access systems every day. However the disadvantage with this

type of authentication is that if you can forget it, and if you write it down people might find it. *Something you have*, a token like a smart card does that you don't have to remember passwords etc. But you always need to bring it with you in order to use it in an authentication process, there is also a chance it can be stolen. *Something you are* for instance a fingerprint, advantages with this is that it is hard to lose, and you as well as with something you have you don't have to be afraid to forget it. The disadvantage with this technology is that it is fairly expensive and is still quite inaccurate. It will be look further into this under biometrics.

There are advantages and disadvantages with all three features, in theory in order to make an authentication mechanism as secure as possible all three features should therefore be included.

The last step in the process is authorization. To authorize means to give approval or permission to something or someone (35). This step in the login process determines who the user is and assign access accordingly, for instance will an administrator of a website have more access than a regular user (34).

A lot of things have been changing the last few years and more than anything how mobile phones are used. The introduction of touch phones and applications has made the login process to something we also have to relate to on an everyday basis.

2.3.2 Biometrics

Biometrics is verification of identity using unique bodily characteristics. It is used as a form of identity access management and access control by recognizing humans based upon one or more intrinsic physical or behavioral traits (38). While hardware tokens, such as BankID, smartcards etc. can be stolen and passwords can be cracked, biometrics relies on your specific bodily characteristics. Biometrics can be divided into two classes, physiological and behavioral. Physiological are related to the shape of the body, for example fingerprints, face recognition, signature, DNA, walking, palm print, hand geometry, iris recognition and odor/scent. Behavioral are related to the behavior of a person. Examples includes typing rhythm, gait, and voice (38).

2.3.3 Adaptive information systems

In order to adapt to the users the system needs knowledge about them. One way to adapt its layout and elements to the users needs, could typically be a context sensitive user interface (39). There are several ways an interface can be adapted to the users needs, it could be adjusted automatically, or the user are in control and adapt it manually. In the sections below three different adaptive information systems, multimodal interface, user controlled management systems and profiling will be presented.

Multimodal interfaces are based on the 'more is more' principle, where the users are offered several ways to experience and control the information through different modalities. For instance touch, sight, sound or speech, or combinations of these techniques like speech and gestures, eye-gaze and gestures or pen input and speech (13)

According to Sharon Oviatt (2002) it is an assumption that multimodal interfaces can “support more flexible, efficient, and expressive means of human-computer interaction, that are more akin to the multimodal experiences humans experience in the physical world (13)”. Vision processing and speech is the most common combination of technologies used in multimodal interfaces. Other reasons to introduce multimodal interfaces are to design for the broadest range of users and contexts of use. All modalities have strengths and weaknesses, for instance will a speech or sound interface not work so well in a public space if the user want to keep the information secret, but in a situation where the user is alone or are wearing headphones or are just not able to look at the screen, an interface like this could be preferred. Offering the user to choose between several modalities will make the interface more robust as the strength of modalities can overcome the weakness in others.

There are some challenges when it comes to multimodal interfaces, since it rely on recognizing aspects of a users’ behavior it is much harder to accomplish and calibrate than single modality systems. Two questions that appear is what do we gain from combining different input and output, and is it really natural to communicate with a computer in the same way as humans communicate with each other (40)?

In a multimodal interface it is important to address privacy and security issues. Users should be recognized by an interface only according to their explicit preference and not be remembered by default. In order to maintain privacy a user should for instance have the option to choose a non-speech interface in a public place in order to prevent people from overhearing sensitive details like identification numbers or passwords (40).

In *User-controlled identity management systems* the user is in control of how identifiable the person is to a service or other users. Fritsch et al. (39) describes some important implications for this type of identity management systems:

- Users should be enabled to participate anonymously or pseudonymously
- Users decide which of their personal attributes to revealed in which context
- Users might like to keep track about what have been revealed

The idea of this type of identity management raises number of issues, but especially two aspects is important in this context. How do we define adaptive user-profiling information systems? And the issues around usability and accessibility of user-controlled identity management. There is no doubt that system like this are more complex, and thus also more difficult for disabled users to use. However Fuglerud et al. (41) states that there is a need for this type of systems because disabled users ”might have interest in determine when and who should get knowledge about their identity and disability status”.

The third approach to adaptive information systems is *profiling*. FIDIS (42) defines profiling as the process of constructing profiles that identify and represent either a person or group/category/cluster, these two types is called personalized and grouped profiling.

Group profiling aims to be able to support specific groups like blind, deaf, cognitively

disabled and so on. In order to this the profile of the group needs to be defined. What needs the users in this group have, and what possibilities and limitations they experience. Developing and use of personas is a well-known method to get to know a user group (23). But there are issues that need to be taken in consideration. When constructing a group profile it is necessary to generalize, many user groups are very heterogeneous which means that it is hard to cover the needs of everyone. Group profiling can therefore be used to exclude rather than include people with disabilities (39).

Personalized profiling means that systems can be adapted to meet the individuals needs (39). User profiles or personal profiles are personalized with a collection of user preferences and data. A personalized, cognitive profile could require sensitive medical data about the type of cognitive disability. This type of data would have to be treated carefully. According to Fritsch et. al (39) extensive use of personalized profiles may lead to uncontrolled proliferation of personal data. A personalized profile can contain information about a person's medical health or disabilities that the person might not be aware of. Another issue is that the person might be unable to stand up for its right for privacy.

Privacy and security can be looked at as two things of the same coin. When talking about the login process and authentication mechanisms security is a central term that should be mentioned. With privacy means protection of information about individuals and other entities. The decreasing cost of storage combined with the increase in communication devices, including and particularly mobile ones, has lead to remarkable impact on personal privacy within a short period of time(14).

2.4 Accessibility

Sharp, Rogers and Preece (13) explains that the area of accessibility refers to the degree to which an interactive product is usable by people with disabilities. The definition of disabilities may vary, but the World Accessibility initiative (43) refers to disabilities as auditory, cognitive, neurological, physical, speech, and visual impairments.

A person is considered to be disabled if:

- They have a mental or physical impairment.
- The impairment has an adverse effect on their ability to carry out normal day-to-day activities.
- The adverse effect is substantial and long-term (meaning has lasted for 12 months or for the rest of their life).

Everyone can be considered disabled; it depends on age, illness, experience and context and changes over time. This project will limit the focus to two types of disabilities, cognitive and visual disabilities which be presented in the next sections.

2.4.1 Cognitive disabilities

2

According to the Norwegian dyslexia association about 5% of the population in Norway has specific reading and writing difficulties, ie dyslexia. In addition there are more than 20% of those between 16 and 20 years that are experiencing general reading and writing difficulties. The characteristics of people with cognitive disabilities are problems involving memory, concentration, reading and writing. In other words cognitive impairment causes difficulties with processing information. This means selecting, understanding, store, retrieve, reason and communicate in relation to the information received. A person with cognitive difficulties has often a combination of several problems, and the extent of the problem varies. Disabilities can be either temporary or lasting. Typical challenges within ICT can be that users forget the pin-code to the internet bank, and a lot of web sites can be confusing and require a high level of attention. In general advanced reading skills are required in order to take advantage of the internet (23).

In the document "cognitive accessibility of webpages and websites" Halback et. al gives a long list of concrete examples and guidelines on how one can present content for users with cognitive challenges(23). Several of the guidelines are small adjustments that probably don't take much time or recourses to implement. A lot of the guidelines point to how the textual content is written and not only how to develop a site for more accessibility. Even with such small adjustments users with cognitive disabilities can experience significant improvements. Following these guidelines will improve the user experience for a lot of people, not only users with cognitive disabilities. One other user group that faces huge challenges regarding ICT is not surprisingly blind and partially sights.

2.4.2 Blind and visually impaired

According to numbers on the Norwegian Association of the Blind and Partially Sighted – NABP there are about 130 000 Norwegians with so impaired vision that they are considered visually impaired and more than thousand Norwegians are completely blind (44). Visually impaired constitute 25% of the disabled population in the world. With over 80% of our sensory impressions perceived through our eyes it is easy to understand that this group of people is experiencing a lot of challenges in their daily lives, and certainly also in the meeting with internet and ICT. The internet today is largely characterized by lack of control, information is designed as suitable for the designer. The last few years there have however been taken initiatives to get at least the content providers to follow standards that make information more available. W3C is the leading agency in this work, and it is now expected that at least all public information comply with their standards (45).

Visually impaired often become disabled because the conditions are not adapted to this user group. What many don't realize it that often small adjustments are enough to improve the accessibility. The NABP have, based on W3Cs Web Content Accessibility Guidelines, created a set of guidelines targeting accessibility for visually impaired(45).

2

<http://www.dysleksiforbundet.no/no/dysleksi/Ofte+stilte+sp%C3%B8rsm%C3%A5l+om+dysleksi.9UFRjG1S.i>
ps

Just as for guidelines for cognitive disabilities a lot of these guidelines are small simple fixes that can be done doing changes in the text or small adjustments in the CSS or HTML-file. When using the internet blind and visually impaired uses ordinary PC solutions, what is special is the implementation with optional software and accessories. So called assistive technology.

2.4.3 Assistive technologies

When talking about accessing technology one can separate between direct access and assistive access (46). The term “direct” access can be described as “adaption to product designs that can significantly increase accessibility” (46). An advantage with this approach is that it increases the ability for users with mild to moderate disabilities to use systems without any modifications. This is in contrast to the term assistive access that indicates access through add-on assistive software that provide specialized input and output capabilities.

Assistive technology describes technology used by individuals with disabilities in order to perform, functions that might otherwise be difficult or impossible. According to University of Washington, assistive technology can include “mobility devices such as walkers and wheelchairs, as well as hardware, software, and peripherals that assists people with disabilities in accessing computers or other information technologies.” Blind or visual impaired persons need to use screen readers or screen magnifiers, while people with limited hand function may use a keyboard with large keys or a special mouse to operate a computer (47).

There is large variety of assistive technology available today; however using assistive technology is no guarantee of being able to access information technology. In order to benefit from the use, the technology is depending on IT products designed and created in a way that allows users to access them. Because of the large amount of assistive technology that works in different ways it can be hard to get an impression of how the information is presented to users with disabilities. This is essential information to know in order to develop the best solutions to the users. However, as mentioned there are several guidelines and standards provided by W3C of how to create accessible design that will facilitate the use of assistive technology(11,26).

As with all users, the needs of users with disabilities varies a lot, and there are many disabled users that do not use any form of assistive technologies, and that can benefit from only small changes in the design. People using assistive technology will despite of this also benefit from software that responds better to their interaction needs (46).

2.4.4 Universal design

Is also called inclusive design, design for all, digital inclusion, universal usability = making technology available, usable by all people whatever their abilities, age, economic situation, education, geographic location, language, etc. (43). Universal design can be described in several ways but at the end it all comes down to one thing, making something accessible to as many as possible. We can talk about universal design in many different contexts, for instance physical things like buildings. In this paper the term will be used in context of information

systems, and design of interfaces on mobile and web technology.

The ACM Code of Ethics (48) states:

“In a fair society, all individuals would have equal opportunity to participate in, or benefit from, the use of computer resources regardless of race, sex, religion, age, disability, national origin or other such similar factors.”

Ben Schneiderman, which is a leading personality within the field of human-computer interaction, extends the code of ethics and calls it universal usability.

“Universal usability will be met when affordable, useful, and usable technology accommodates the vast majority of the global population: this entails addressing challenges of technology variety, user diversity, and gaps in user knowledge in ways only beginning to be acknowledged by educational, corporate, and government agencies (49).”

The following list gives a more detailed explanation of what requirements there are for universal design. These seven principles were authored by a group of architects, product designers, engineers and environmental design researchers as a guide for design disciplines including environments, products and communications.

1. *Equitable (fair/equal) Use:* The design is useful and marketable to any group of users.
2. *Flexibility in Use:* The design accommodates a wide range of individual preferences and abilities.
3. *Simple and Intuitive Use:* Use of the design is easy to understand.
4. *Perceptible Information:* The design communicates necessary information effectively to the user.
5. *Tolerance for Error:* The design minimizes hazards and the adverse consequences of accidental or unintentional actions.
6. *Low Physical Effort:* The design can be used efficiently and comfortably.
7. *Size and Space for Approach and Use:* Appropriate size and space is provided for approach and use.

These principles are intended to apply when evaluating existing design, but they should also be used as a guide from the beginning of a design process. They aim at educating both designers and costumers, and learning them especially about characteristics of usable products and environments (50). When the goal is to create universal design these principles are good to use as guidelines. They might not be relevant to all design and does not describe how to solve design issues in practice, but can help you in the right direction.

2.4.5 WAI

World Accessibility Initiative (WAI) is an initiative started by W3C working on developing guidelines and standards for Web accessibility (10). In addition to working with the web in general they have also been looking into the mobile web in particular and how to make a web

site accessible both for people with disabilities and for mobile devices (43). By combining and follow the Web Content Accessibility Guidelines (WCAG) and the Mobile Web Best Practices (MWBP) (26) W3C states that your web content will be more accessible to everyone regardless of situation, environment, or device.

2.4.6 E-inclusion

The e-inclusion policy by the European Commission aims to achieve that “no one is left behind”. It focuses on participation of all individuals and communities in all aspects of the information society, and is defined as “inclusive ICT and the use of ICT to achieve wider inclusion objectives”. With this policy the European Commission “aims at reducing gaps in the usage of ICT, and promoting the ICT usage to overcome exclusion, and improve economic performance, employment opportunities, quality of life, social participation and cohesion” (51). As Norway is not a part of the United Nations this policy does not directly apply here. However, there have been created a proposal for a regulations about universal design of ICT, and they are currently being prepared by the Ministry of Government Administration and Church Ministry. As soon as the regulations are ready they will be sent for public consultation and the Ministry aims at implementing them by 2012.

§ 11 in the Anti-Discrimination and Accessibility Act, is based on the same principles as the e-inclusion policy, and aims a preventing discrimination on the basis of disability. The act first and foremost refers to ICT solutions that support the company’s normal functions and the main solutions directed at or made available to the public (52). According to the current draft of the act the University’s home page will be included while the internal case management systems would not. The act does not include ICT-solutions where the design is regulated by other laws which is the case for internal systems in a company or at schools and educational institutions where the §12 Duty of individual adaption apply (53).

The current draft of the act only includes network web-solutions and vending machines. In this setting ICT-solutions are defined as technology and systems that are used to express, create, convert exchange, store, reproduce and publish information, or otherwise make information usable. Vending machines are defined as machines or other devices which the user operates alone to by a product or perform a service. Web services or online solutions are the dissemination of information or service that is available in the browser or equivalent, accessible via URI (Uniform Resource Identifier) and using the http protocol (Hypertext Transfer Protocol) or similar to make content available (54).

As mobile phones account for a large part of the internet traffic and that the mobile users are about to pass desktop internet users(2) makes it interesting to look into how anti-discrimination and accessibility act will affect the design on mobile devises. A question to ask is how to define the company’s normal functions and main solution. A web services in not often bound to one specific device. Looking at internet banking several banks are offering their costumers to use their touch phone as a security token when accessing their internet bank. The banks main solution rely on several devices and the phone become a part of the

normal functions and according to the definition, the act would also apply to the banks mobile solution. There technology is rapidly evolving and the answer to what a main solution and normal function of a company is will probably change. Companies could also have several main solutions, for instance could both ATMs and a banks web services account as a part of the company's normal functions.

As long as the draft regulations has not been in a public consultation and not formally adopted it is not possible to get specific feedback on whether or not a solution will fall under the obligation of universal design. To decide whether or not a mobile web solution or native mobile apps will be included in the duty of universal design must be assessed on the basis of the current definitions of ICT solutions, vending machines and web services or online solutions (54). Current ICT-solutions that are included in this act have to be universally designed within 2021 while new ICT solutions that are created after the approval of the regulations have to be universally designed within 12 months.

3 Methods



Figure 3.1 Dilbert by Scott Adams (1995-11-08)

In this chapter I will describe case study and present the methods used for gathering data. I will start with presenting the case study which have been the framing the research.

3.1 Case study

The framework for my research is case study. Robert E. Stake (55) defines a case study by interest in an individual case, not the method used. In other words, it is not a methodological choice, but a choice of what to be studied. A case study can consist of either one single case or a collection of several cases, focusing on either the specific case or on an issue (56).

This study is chosen to be an instrumental case study, which means that the case is examined mainly to prove insight into the issue or to redraw a generalization (55). The case used in this research supports and facilitates the understanding of authentication on touch phones. Feide is examined in details but all because this helped to pursue the external interest (55).

Coming to understand a case usually requires extensive examine of how things gets done. It can be hard to define the boundaries of a case. Where does the case end and the environment begins? The case is organized around the four research questions presented in the introduction. This scope of the case and this project is described in some manner in the introduction under delimitations, and will be further described in chapter four, *Case*.

A case study is both a process of inquiry about the case and the product of that inquiry. Even though this is a singular case it has several subsections. There are different groups of people involved, first and foremost employees at the University and students which can be divided into disabled and non-disabled. In addition the case is present in different occasions; school days, holidays, close to deadlines e.g. Each of these does also have its own context. The term context how is elaborated in chapter 2, *mobile context*.

The case is an opportunity to study and learn from a phenomenon (55). As there is a naturalistic approach to this study I seek what is ordinary in the case, in order to detect and study the common.

3.2 Qualitative research

This thesis are based on qualitative research. A case study in not necessary a qualitative study, but it is a common way to do qualitative inquiries (55). In an attempt to go into details of the topic I have been in contact with activities and operations connected to the case, and reflected and revising concepts and theory related to the it to learn more and get a good basis to answer the research questions (55). To get a full overview it has been important to look at both social, situational, and contextual aspects of the case.

Opposite from qualitative studies, quantitative studies, facilitates in principle not generalization, but can generate an in-depth understanding of peoples behavior and why they behave like they do.

3.3 Ethics

In all types of qualitative research one will have to consider various ethical issues during the collection of data and in analysis and dissemination of qualitative reports (56).

- Protecting the anonymity of the informants.
- Disclosing (or not) the purpose of the research?
- Deciding whether (or how) to use information shared “off the record” in an interview in a case study.
- Determine whether the researcher should share personal experiences.

Since the informants were asked to share their personal experience of security and details about their use of different terminals, the information they provided can be characterized as sensitive and their contributions have during the entire project have been kept anonymous. The involved parts were all informed about the purpose of the research in front of their participation and were also given the opportunity to withdraw from the study at all times. All the findings in this project are generated from the methods that have been used and I have chosen to not include information that have been shared “off the record”. There were kept a relative informal tone during the interviews, but I tried not to influence the informants by sharing my own experiences, but

How qualitative data is organized and stored is important. Creswell presents some principles that are especially well suited for qualitative research (56). I have made a list of considerations to take, based on his principles, however these are somewhat outdated as we use a different technology for recording and storing data today then we then. Which is why I have updated the list to make it more suitable for today’s technology.

- Always develop backup copies of computer files (Davidson, 1996).
- Develop a master list of types of information gathered.

- Keep the data in password protected files.
- Use high-quality equipment for audio-recording information during interviews.
- Protect the anonymity of participants by masking their names in the data.

I have followed these recommendation through out the project, and the data will be deleted after completion of the research.

While gathering data in this project I have followed the triangulation strategy. According to Sharp, Rogers and Preece (13) triangulation means using more than one technique to tackle a goal, or using more than one data analysis approach on the same set of data. I have used cultural probes to uncover people's relationship to security on touch phones; this was followed up by interviewing some of the participants, and in addition to this eye tracking were used to test out different authentication mechanisms. This provided different perspectives and enabled me to uncover multiple layers of usability and accessibility issues by looking at the findings across the techniques. Triangulation can in many ways make the research gain credibility (55).

3.4 Cultural Probes

The first method used to gather data was cultural probes. Patrick Kennedy (57) uses the analogy of a space probe like Voyager to describe probes, «it is something that goes somewhere were we can't go our selves and transmits back data». This is exactly what it was used in this project, the probes were sent out together with the participants for about one week and were supposed to evoke responses and feedback for me to use in the research. This method is called cultural probes because we look at culture in terms of peoples beliefs, how they act and behave.

The probes were twelve paper cards bound together with a tread (Appendix C).

- *About the project*: a short introduction of the project.
- *Three questions (x3)*: three questions about how the phone was used, any irregular happenings? How many times did you use your phone to login to external services. And where did you login?
- *Photos*: Take a couple of pictures each day to document what context you use your phone in and send them to me by mail.
- *Your phone*: What screen lock do you use? Mark on a scale how secure you experience the content on your phone.
- *Security - computer*: Mark on a scale how secure you experience different authentication mechanisms to be on a computer.
- *Security - smart phone*: Mark on a scale how secure you experience different authentication mechanisms to be on a smart phone.
- *Notes*: An empty card to note down additional comments.

- *Consent*: Information of how the data would be used. The participants needed to sign to confirm this.

The cards and the pen were given to the participants in an envelope. The size of the cards was important, they were only a little bit larger than an iPhone, I wanted people to be able to bring them with them all the time, and then it was important that they not were too big. A pen was tied to the card with a thread, so that the participants always would have a pen available if they wanted to write on the cards. In addition to this on one of the cards referred to a webpage where there was more information about the research ³.

To get as much feedback as possible it was important to create a design that invited the participants to fill in answers. In order to achieve this I used elements like checkboxes and text fields and progress bars that the participants would fill out. These were elements that most people would recognize from forms on computer applications and websites. Prior the main study I conducted a pilot study in order to make sure that the probes would be viable. As Sharp, Rogers and Preece (13) mentions, participants can be and usually are very unpredictable, even when a lot of time and effort has been spent planning the data gathering session.

A pilot test is a small-scale rehearsal of a larger research. It gives the researcher the opportunity to discover errors and make changes, it is cheap, and does not demand a big effort. Including a lot of people in user testing is both time consuming and expensive and the researcher cannot afford the consequences of errors and mistakes. Pilot studies are excellent for training inexperienced researchers allowing them to make mistakes and errors without failing the project. It is important to report from the pilot test, so that the same mistakes are not repeated in later studies. A pilot study makes it easier to make logistical and financial estimates for the main study (58).

I used my supervisor in the pilot test. This way I could gather data and also get feedback from an expert on the shaping of the probes. The probes were in Norwegian as the people I would use in my research most likely would be Norwegians. The impression I got from the pilot test was that it worked fine. I got them back after five days and the cards and the pen were still tied together with a thread. In addition to filling out the cards he also suggested some changes in the wording and order of the cards. The cards did not need to be filled in any specific order, but the question cards with three questions on them, should be filled out one each day, because of this it would be natural to add them to the beginning of the stock.

I could see that some of my ideas about the cards did not work out the way I planned. As mentioned I was inspired by the progress bar where one should mark out what level of security you experienced with different types of authentication. The pilot test was not filled in like a progress bar, but he rather just made one mark on the line. The metaphor was obviously not

3

www.folk.uio.no/siribst/MasterResearch

as clear as I hoped, but I was still able to get the information I wanted from it, and saw therefore no reason to change it.

Assuming that the test person had a touch phone with camera, one of the cards asked the participant to take pictures of where the phone was used. They were encouraged to take two or three pictures each day. I received only five pictures, but the pictures together with the rest of the answers gave me an impression of how the phone was used during the five days the test lasted.

In the main study the cultural probes were handed out to 10 students from the institute of informatics at the University of Oslo. They were explained a little bit about the project, but were basically left to themselves and the instructions on the cards. It took between one and two weeks to get all the cards back. I received a lot of images on mail, but did also had to remind some of the participants to send them. There were a lot of interesting findings from the probes, and this formed the basis for the interviews.

3.5 Interview

The first step in the interview process was to create an interview guide. This contained some main topics, and some supplementary questions for each of them. In addition to this I presented some of the results from the probes by graphs and pictures to facilitate a discussion about the result and different authentication mechanisms.

First I conducted a pilot interview, which generated some indication of how the interview could be improved, and made some changes before I conducted five more interviews. The interviewees were students that had participated in the probe study and had agreed to be contacted for a follow-up interview. The interview was focusing on much of the same things as the probes, peoples understanding of security on touch phones, and how that affects our authentication habits. In contrast to the probes, interviews gave an opportunity to go deeper into the subject and apply additional questions to follow up on what was being said.

The interviewee signed a consent (Appendix D) describing the project and the interview. The interviewee was also informed that the data would be treated anonymously and that their identity would not be revealed in any reports based on the interview. The interviews was recorded with an iPhone, but if the interviewee decided to withdraw all data including the recording would be deleted.

I created two different interview guides (Appendix E), the initial questions were the same, but one interview guide was directed towards people that had answered that they had a screen lock on their phone, and the other to people that did not have a screen lock. The interviews were semi-structured combining features from both unstructured and structured interview with closed and open questions. The interview guide was used to make sure the same topics were covered in all of the interviews (13). The interview started with some initial questions about the interviewee and its background, then followed up with questions within the topics mobile

usage, computer usage, a bit about the responses on the probes and then a bit about ‘the cloud’. The interviews were conducted at the University, in familiar environments for the students.

3.6 Eye tracking

User testing has proved that there often is a difference between what people say they do and what they actually does. Using the eye tracking equipment Tobii X60 & X120 Eye Tracker, provided by the Norwegian Computer Center I tested the current version of Feide on a mobile device. “Tobii is the world’s leading vendor of eye tracking and eye control technology (59) providing systems and software used within the scientific community and in usability and market research, to analyze vision, human behavior, user experience and consumer responses.” The equipment is designed for use in office and home environments, but does not give the user the opportunity to interact with it in a completely natural way as it is mounted on a stand, and not held by the user. The user can rotate it to switch between horizontal and vertical view.

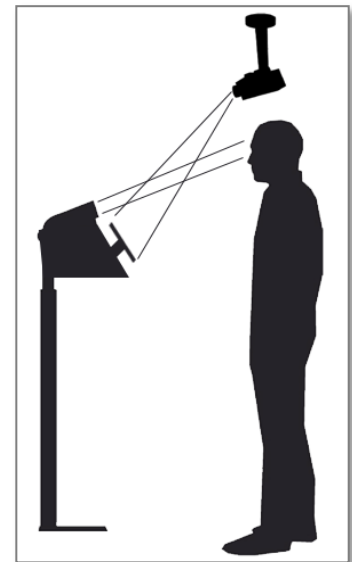


Figure 3.2 Tobii Eye Tracking

While an interview is a human to human interaction, user testing provides data about the human computer interaction. Observation and think aloud are regular methods used to study human computer interaction, but the disadvantage with these methods is that they does not provide information about what users are doing in between clicks and keystrokes (60). By using an eye-tracker it is possible to “capture precisely where users are looking on a display over time”.

Eye tracking gives the researchers a unique opportunity to see what the user sees, and according to the mind-eye hypothesis (7) people are usually thinking about what they are looking at. This does not mean that they always understand and engage with it, but it indicates at least that they are paying attention to it, especially in cases when the user are focusing on a particular task (7). It is therefore reasonable to say that fixations equals attention and are normally placed on elements that people are concerned about. One can also probably conclude that the longer the fixation lasts, the more the user think about the element. It is important to note that eye tracking does not reveal *why* users look and think about design elements.

Reasons why people look at certain design elements can be that they find it relevant and interesting or it could be the complete opposite, that they think it is confusing and hard to understand. It can also be usefull to note witch elements the user are not looking at. People tend to overlook items that don’t seem clickable or useful to them. If the people are familiar with the interface they does not waste time on items they don’t need. This could for instance be navigation elements that are repeated on several pages within a site. As Nielsen and

Pernice (7) writes; “the web is too big for users to attend to everything, and those sites that allows them to focus on what they want are the ones that people returns to”.

Tobii’s technology is based upon the principles of corneal reflection tracking, and have enabled non-invasive tracking of people’s eye gaze. By using infrared light a video sensor can detect the cornea and the dark spot of the pupil. These are again used to calculate the orientation of the eyeballs and triangulate their on-screen targets (60).

The e-Me research project (61) have created and tested a prototype on elderly users. The prototype is a web solution built with HTML, CSS and JavaScript. It present five different authentication mechanisms, image, password, sound, question and pattern (62). The users first arranged the mechanisms in preferred order, they then went through several steps registering the methods. All of them introduced with a short description and some also with an example. At the end the users were asked to rate the authentication mechanisms based on how well they liked the different alternatives. The ratings were from 1 to 5, where 1 was very poor and 5 very good.

Different from the previous testing the prototype was now tested on a mobile device instead of a computer. The biggest change was that the interaction with the system went from holding a mouse and typing on a keyboard to using fingers on a touch screen. A challenge was also that the prototype was not optimized for the size of a mobile screen, and only worked optimally in Internet Explorer. Because of this the users were for instance not able to drag and drop the authentication mechanisms to change the preferred order which was the first step in the prototype.

Prior the testing I participated in a course to learn how to use the equipment and prepared a couple of assignments that the test subjects would perform. The students used their own touch phones during the testing, this were convenient as the users were familiar with the OS and did not need time to adapt to a new interface. The first task the user conducted was to enter www.uio.no, and login to Vortex using their Feide login details provided by the University of Oslo. The second task was to go through the test scenario with different authentication mechanisms in the e-Me prototype. Both tasks were followed by some questions of the users’ experience, the interaction and security of the different methods.

Five students participated in the testing, their age varied from 23 to 26, and they were all master students in design, use and interaction from both first and second year. Some of them had participated in in the probe study, some had also participated in previous interviews while for the rest this were their first introduction to the project. Each session lasted for about 30 minutes and took place at the Norwegian Computing center (NR), next to the institute of informatics.

After doing the user testing with the screen capture and eye tracking, visualization of the data was created with the Tobii Studio software. Eye tracking generates a lot of data, and there are many ways they can be processed and presented. Heat maps is one of them, showing the

combined fixations of many users on a page, and highlighting areas of high frequency with red. For a web page Nielsen and Pernice recommend to include data from at least 30 users to create an effective heat map (7). Another way is gaze plots which only display a single user's eye movement, and representing each fixation with a dot and the saccades between them as (7).

4 Case



Figure 4.1 Dilbert by Scott Adams (2005-08-02)

This chapter presents and describe the case, research projects and participants that have been included in this study. There will first be given a short presentation of the research group, e-Me and one of their projects where they were working with alternative authentication mechanisms. In addition to e-Me I have been in contact with the Norwegian Center for ICT in Education as they are closely connected to Feide which is the case I have been focusing on.

The primary objective of this thesis has been to provide new knowledge within the field of accessible authentication on touch phones. I have contributed by doing research on existing authentication solutions within the educational sector in addition to expanding the e-Me project by approaching another platform and a different user group then what have been included in the research until now.

4.1 e-Me

The research project started out in May 2010 and ends in 2013. The project is financed by the VERDIT-program in the Norwegian Research Council and is owned by The Norwegian Computer Center (NR) while Karde AS leads the project. In addition to this there are partners involved from Tellu AS, the Department of Informatics and the Department of Private Law at the University of Oslo.

The e-Me project is focusing on inclusive identity management in new social media, and are working to obtain knowledge within this field (61). The background of the project is a growing need for easy-to-use, accessible and universal designed authentication mechanisms. NR states that it for a long time have been an issue that simple and accessible use of electronic services has been ignored due to security reasons which is also the case within new social media.

All their empirical research is related to specific cases about privacy and security for users with functional impairments. The case organizations, which are Encap AS,

Brønnøysundsregistrene and Storebrand, provide issues to the projects. While the users' challenges are studied in collaboration with user organizations, Blindeforbundet, Dysleksi Norge and Seniornett Norge (61).

The research project will achieve new knowledge within this field by among other things to do research, surveys, prototyping, and user testing. One of the products that have been developed from the project is a prototype with five different authentication mechanisms.

4.1.1 Prototype

The goal with the prototype was to find authentication mechanisms that were secure, and at the same time accessible for people with visual impairments, cognitive disabilities and memory problems. If it would be an advantage with mechanisms where the user does not have to remember and write a password. The prototype were programmed for working in the desktop browser Internet Explorer. By testing the prototype on elderly from NABP, the Norwegian dyslexia association and Seniornett⁴, observing and interview them and ask them to rank the mechanisms based on ease of use their goal was to identify advantages and disadvantages of various mechanisms for both disabled people and people without disabilities (63).

The prototype consisted of five authentication mechanisms, password, recognition of images, sounds and pattern and personal questions. The research made it clear that the use of sound and image recognition were more complex then expected. The level of difficulty increased with the number of images and sounds. Regarding the sound authentication they found that there were maybe too many impression to keep track of, and there would also often be a need for headphones in order to avoid unauthorized people to hear the sound (63).

The research showed that what was most important for the elderly the sense of safety and recognition, more then the time they used. Even if the authentication with questions took longer time then the other methods it was questions and passwords that was preferred by the elderly. Both were something they had used before and recognized and therefore perceived as safe. The pattern were easy to get to know and understand, but as this was a new unknown mechanism for them it was perceived as less safe (63).

⁴
<http://seniornett.no/>



Figure 4.2 e-Me prototype

4.2 The Norwegian Centre for ICT in Education

The Norwegian Center for ITC in Education are working to ensure better integrating of ICT, for increased quality, improved learning and better learning strategies in education. They are targeting children from kinder garden and up to high school in addition to teacher students (64). The centers projects are closely connected to Feide, and are supporting the implementation and basic training of this solution so that the benefits increase for the schools and students.

4.3 Feide

Feide (Common Electronic Identity) is a solution for secure identification to educational web services in Norway, chosen by the Ministry of Education and Research (65). As OpenID, Feide is based on the idea of Single Sign On (SSO). The user do not have to register new user accounts on several different services, and therefore don't need to remember many sets of user names and passwords.

Feide states that the technology simplifies the process for all parties involved by using so called federated identity management which is based on the concept that services rely on user authentication at the user's home organization (65).

- The user register once at the *home organization* where he is affiliated. For instance a university.
- The University saves the personal data and gives the user log-in details.
- When the user wants to enter a service that require him to log-in with the Feide solution. The University checks the applied information with the saved personal data and sends the status back to Feide that reports to the service.
- The service gives the user authorization to access based on the details received from the University.

- The user has to accept that the details are given to the service to be able to log-in.
- On the log-in page the user can see what type of information that will be transferred if the authentication is successful.

In addition to this Feide also provides Single Log Out (SLO) of usability and security reasons. With this function you get feedback on what services you are logged into with Feide, and can chose to log out from one or several at the simultaneously (65).

Feide have provided me with a list of all the services at the University of Oslo that are connected to their identification solution (Attachment A). Note that this list does not separate the services that are available for employees and students, as Feide did not have a complete overview of this.

Feide is currently used mostly on services adapted to desktop browsers, but they have also enabled Feide login for mobile applications. This works in such a way that the application uses a web page to handle the authentication dialogue (66). The University of Oslo does not have an official app, and very few apps have implemented this solutions. I have in this project therefore focused on the existing solution that is available to students, which is login through a mobile browser. Feide is constantly expanding and the user base is increasing rapidly, and they are also working with improving the technology. At a seminar organized by e-Me a representatives from the Norwegian Center for ITC in Education presented a pilot project called Tabia. This was a project focusing on making web content more accessible by enable the users to specify their personal preferences.

4.3.1 Tabia

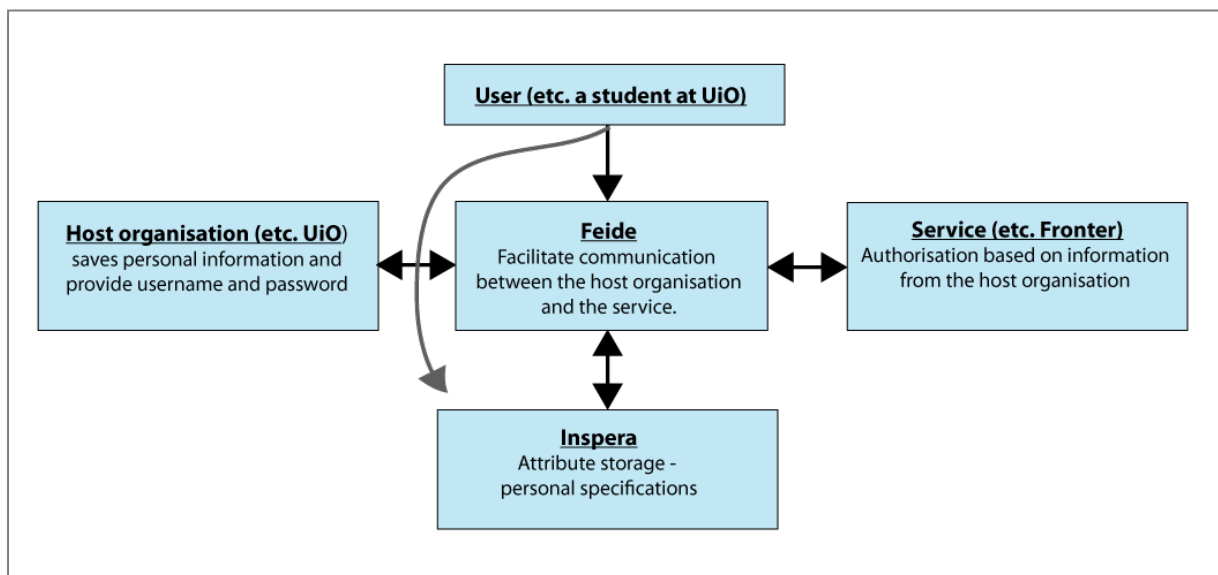


Figure 4.3 Feide login connected to Inspera attribute storage

In the Tabia project Feide and the Norwegian Center for ITC in Education have been working on in cooperation with a consulting firm called Inspera. The concept were tested on TV2

Skole which is a web site and learning tool that every weekday delivers news broad casts, film events and tasks directly related to core subjects in primary and secondary schools and adult education(67). The purpose was that the user should be able to specify if the person wants to have the content adapted to the persons needs. If the user is have a hearing disability he might prefer to watch videos where the information is translated into sign language. Other visitors might want the letters to be bigger or in a certain color because of visual impairments. In Tabia there are added a list of attributes where Feide would be able to get the users preferences, by a string of numbers, without recognizing the persons, and communicate them to the service which then adapts by the defined attributes (68).

While Tabia only focused on making web content accessible in desktop browsers, my approach is aimed towards the authentication process.

4.4 Feide on touch phones

In Norway it is important that everyone have the same opportunity to take higher education. Therefore the University is required to offer individual adaption in teaching and examination for students with special needs if they claim it. The internet is the most important communication channel between students and the educational institution, and a lot of information are only available for the students online. This imply that the students rely on internet connection in order to follow a study program. Reserving a book at the library, accessing mail and checking course information is examples where one need internet access.

With the evolving mobile technology many students uses their touch phones also in the educational context. As described in the introduction mobile phones generated about 10% of all internet traffic in 2011. This mean that there are much at stake, and that there are a lot to gain from adapting web services to mobile phones. There are no reason to believe that this trend is any different for educational web services, which is why this is important to look into.

To set the stage for this case I have created a couple of scenarios that describe situations where authentication on mobile phones would be used.

“John is sitting on the subway on his way to the University. He remember that he have forgotten to renew the loan period on the book he rented at the library, and uses his touch phone and Feide to login to Bibsys and renew it.”

“Jenny is in a lecture, when the professor reminds them to approve their curriculum at Studentweb. She decides to do it immediately before she forgets it, and use her touch phone and Feide to access Studentweb.”

“David was surfing on his Facebook with his phone in his lunch break and saw a posting about the election for the student parliament. He clicked the link and logged in with Feide to vote right away.”

These scenarios are inspired from my five as a student, and are based on actual events. They presents the variations within the mobile context and say something about how mobile

devices are used among the younger population.

4.5 User testing

The e-Me prototype were used as a part of the user testing. The goal was to get insight in how the different authentication mechanisms worked on touch phones in practice with real users. The users were observed and their eye movements were tracked while they tested the prototype. This was done to uncover usability problems, but the users perception of the different methods, which one they prefer and why was also emphasized.

In addition to the prototype Feide login were tested with the same approach to see how password work as an authentication mechanism on touch phones and how a service originally intended for a larger screen would work on a small touch screen. How the testing were conducted was be described in the method chapter, and the findings will be described in chapter 5.

4.6 Students

The participants that were included in this study are all students from the Institute of informatics at the University of Oslo. Throughout the project 11 students, with age ranged from 23-29 years, were involved in probes, interviews and testing. They were all at current time in their fourth or fifth year in their study of informatics, experienced students and familiar with most of the ICT services that the University provide. Accessibility to the users were important in the choice of participants, but it was also essential that the informants had access to Feide login.

There are both challenges and advantages with having students as the user group in this case. One challenges is that now a days students comes from a lot of different cultures both exchange students, and people form foreign countries that take their whole degree here in Norway, is increasing the diversity among the students. However there are also several advantages by using students as a target group for this research. There are exceptions but the general age of students is between 18 and 30. Most people at this age are experienced in using computers, as they have grown up hand in hand with technology. Students are used to be in a learning situation and acquiring new knowledge and are early adopters and heavy users of new mobile technology.

Involving users with different background would ensure variety, but not necessary representativeness. The informants can be regarded as expert users since they probably have a greater interest and understanding of technology then the average student. Because of the narrow range of informants and their background, it is difficult to generalize on the basis of this study. They did however not have special expertise within the field of authentication, which means that they do not differ that much from other users after all.

5 Findings



Figure 5.1 Dilbert by Scott Adams (2009-03-10)

In this chapter the results from the probes, interviews and eye tracking will be presented.

5.1 Cultural probes

The first section will go through the findings that were generated from the cultural probes, divided into the themes of the cards. All the replies were in Norwegian and have been translated into English.

5.1.1 Three questions

The informants filled out three questions everyday for five days. The first question was; *have you had any unexpected experiences using mobile today?*

From the period of the informants filled out the probes there were reported in total 16 incidents as unexpected events. In several cases the phone was turned off, either due to empty battery, or unfamiliar reasons. Here are some of the feedback on the question.

- “My phone did not respond when I tried to unlock it”
- “Was not able to connect to the internet so had to restart the phone”
- “Managed to unlock the phone WITH glows”
- “Had to write the password on my e-mail, that is normally saved.”
- “Got a tip about shortcuts on iPhone and hopefully I don't need to type in username and email addresses anymore! :)”

The second question were; *how many times have you used your phone to login with?* Four users did not have a screen lock on their phone, while the rest did and some counted them as logins, because of this the number of logins varies a lot. Some did not note down any logins,

5 Findings

- In addition to these, pictures are taken of events, strange things people saw or things they wanted to remember. I also received some screen shots that were displaying situations where the person were connecting apps or other social media to Facebook for the first time, and had to type in a one time password. In addition to screen shots of the users' first meeting with a new application, where the person either had to register or sign in.

5.1.3 Your mobile

This graph shows the result of how the informants used their own mobile. Four out of the ten people did not use any type of screen lock on their phone, only the slider. On the question of how secure the informant experience the content and service on their phone no one said that they experienced it as very secure or unsecure, but most graded it as medium or a little bit lower or higher then that.

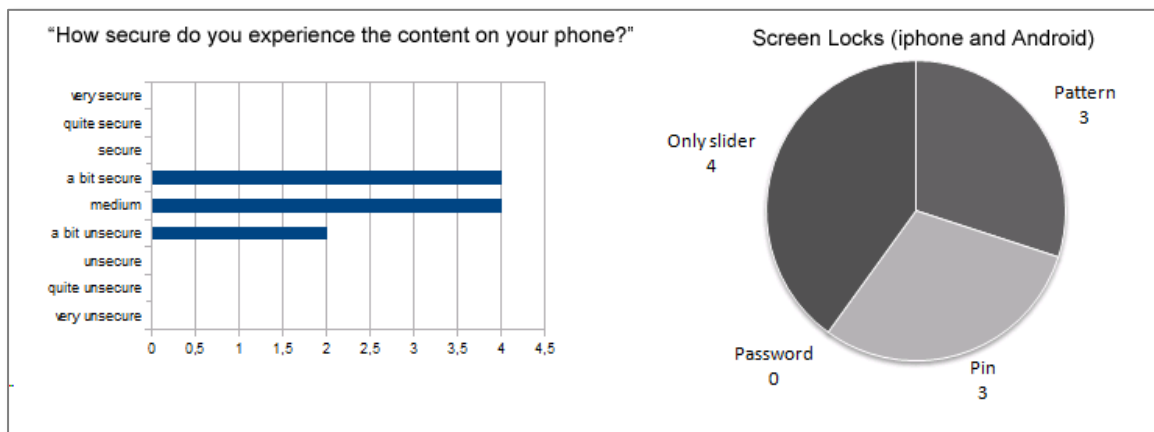


Figure 5.3 Security and Screen Locks

5.1.4 Computer and mobile security

On this card the informant were presented with five different authentication mechanisms, and were asked to mark how secure they experienced their information when using the different mechanisms. The result here were quite spread and but the most common authentication, the

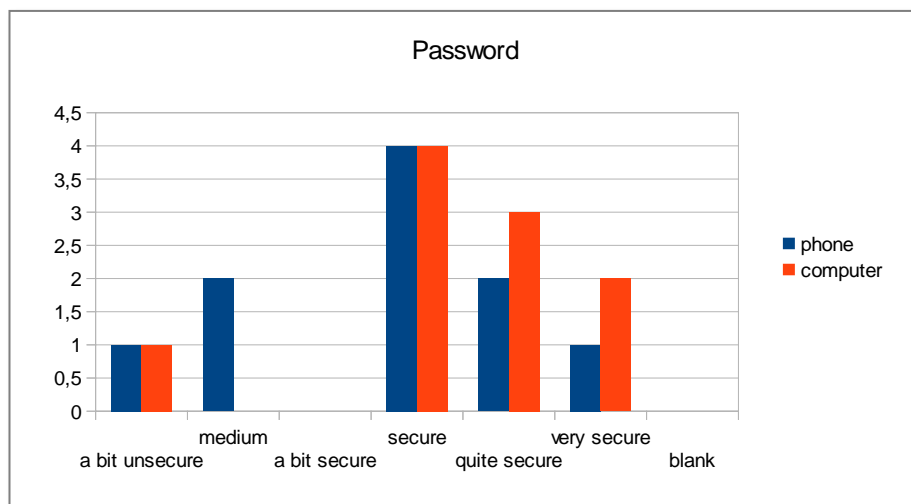


Figure 5.4 Password authentication

password was the mechanism that the informants had most confidence in, both on touch phone and computer. Pin-code which is more common on a touch phone than on a computer the informants experienced as more secure on the computer than on a touch phone. From the graphs it looks like the informants in general feel that the information on their computer is more secure than the information on their touch phone, independent of what authentication mechanism they use.

5.1.5 Notes

It was not specified what the informants should write on this card, but all the comments referred to authentication on touch phones and issues regarding this.

- “Have noticed that I have problems reading the words you have to type in to prove that you are not a computer (CAPTCHA). That makes me annoyed!”
- “Drawn pattern are very safe if strangers take your phone, but people you know have often seen the pattern. That can have disastrous consequences.”
- “Most logins are the code on the phone. Most passwords on apps are saved so I rarely write these.”
- “I don't use pin-lock on my phone in fear of losing the phone and if an honest person finds it, he/she will not be able to call me because the phone is locked.”
- “Security in biometry is depending on where you are, what context. Movement on the tram can for instance be easy to detect.”
- “I was a bit unsure about the question on login on mobile. I have been on several social media with my phone – but I am usually logged in all the time. The same with wireless networks. The password is saved after the first login, so I am logged in automatically. I also use my phone at the same places (and in the same situations – so the pictures will be somewhat similar).”

5.1.6 Summary

The test pointed out that it was a difference between how this person look at security on a computer compared with a touch phone. Authentication mechanisms that the user experienced as secure on a computer was not necessary experienced that secure on a touch phone. All types of authentication were experienced as quite insecure on the touch phones. On the computer the sound combinations were marked as very insecure, a drawn pattern as insecure and the rest over medium. Password which is the most common form of authentication was rated highest of them all as secure. None of them were rated as very secure. An example of an interesting finding was an informant which experienced the drawn pattern as very insecure on a touch phone, in spite of this the person rated the security of the information on the persons phone as medium secure, while using a pattern as screen lock.

5.2 Interviews

The interviewees were conducted with five students of informatics at the University of Oslo, at the age from 24 to 29. Their living situation varied from student apartments, to shared housing and living with a girlfriend or boyfriend. Four out of the five informants were using an iPhone 4 while one had an Android, but there were a mix of people with and without a screen lock on their phones.

5.2.1 Mobile usage

The students feel very dependent on their phone. They use it all the time, bring it everywhere and always keep it close, in their pocket or purse or on the desk at school, table at home and even in the bathroom.

- “I’m 100% dependent; it’s the whole world down in my pocket.”
- “I bring it everywhere.”
- “I use it as an alarm clock; don’t even have a regular clock.”
- “Having access to my mail has made me dependent of it; I’m checking that all the time.”

Of applications that contains personal information the student mentions messages, images, mobile banking, PayPal and all social applications like Facebook, Twitter, Foursquare, Gowalla, find friends, Skype, LinkedIn, latitude. However mail is the service that they consider to contain most personal and sensitive information.

- “If you order a new password it is sent to your mail.”
- “Almost all services are connected to your mail, so if you have access to a mail account you also have indirectly access to a lot of other services.”

Talking about what type of information people do not want to get into the wrong hands applications like Facebook and e-mail were mentioned also here. In addition work-related things, address information, personal information about themselves and their contact list came up.

- “I remember when I lost my photo camera once, and even though it was only pictures of friends and family I felt uncomfortable knowing that people could see my pictures. It’s the same thing if unauthorized people get access to your Facebook.”
- “I have confidential information saved on my phone in connection with my master project, and if that were lost or got into the wrong hands it would be incredible bad.”

On touch phones most people don’t logout of the applications, they just use the back button or closes it without logging out. This makes it possible to access the applications automatically without typing in the username and password every time. The interviewees were asked if they were thinking about the private issues of having automatic access to applications.

- “No, because I think it is stress to login again. I want to have the application available instantly. For instance it is stressful to use the mobile banking app, because I have to

login every time, but if I had to prioritize, I'd say that the bank is more important than Facebook."

- "Well that's the reason why I almost always know where my phone is, or that I bring it with me or keep it under observation."
- "I don't really think about privacy."
- "It is first and foremost, very convenient that you do not have to log in and out constantly."

On the question if there were any services or applications that did not have automatic login, several of the interviewees had to check their phone to see what the status was. All of them answered yes, and apps like mobile banking, PayPal and the Apple ID password were mentioned as examples where you don't have a choice and have to type in the password every time.

- "Since there are payment opportunities on those apps, I would not have chosen automatic login if I could, since that can get greater consequences."

Only one of the informants had lost or been robbed their phone. There were no screen lock on the phone, but the informant tried to remotely delete the content. However as the phone was turned off at one point the informant was not completely sure if this worked. To limit the access to the apps, all passwords were changed just in case. The other informants had not experienced their phone to get lost or stolen, but were aware of the risk and had some thought on what they would have done if it happened.

- "I would have tried to find it again with some tracking software, and done a remote wipe of the content" (iPhone user)
- "I'd rather delete the content on my phone remotely then lock the phone and SIM-card. For instance: I'd rather risk paying 10 000 NOK because someone calls to Africa then have someone access my mail, Facebook, messages and contacts."

They also had a theory of why they had avoided losing the phone.

- "I feel that I know where it is at all times, and automatically check where it is from time to time. Like; is it in my pocket where I put it earlier?"

5.2.2 Computer Usage

The next topic of the interviews was computers and screen locks. Several felt the same need for screen locks on computers as on the phone, but dependent on the context and situation the need for a screen lock changed. The students stated that they lock the computer at school or other public places, but not at home.

- "I lock my computer at school, not because I'm afraid that people would see what I was working on, but because I want to avoid friends and other students playing with my Facebook profile for instance."
- "Some businesses have it in their guidelines that the computer should be locked if it is

5 Findings

left unattended, but I have to admit that I did not always do that, I had colleagues in the same office and trusted them to keep an eye of it, but I should probably have locked it to be completely sure it was safe.”

In a web browser the users often get a question if they want to save the username and password for the service that they are using. The interviewees were asked what they do when they get this question.

- “I have saved the password on Facebook, but on services that I don’t visit that often I don’t save it. I don’t see the need there, and it is easier to type in the password on a computer than on a phone.”
- “Google chrome remembers my user name, and I use the same password with some modifications almost everywhere, it’s not so stress to write the password on a computer as it is on a phone.”
- “I’m aware that my services are less secure if I have saved the password and username, however, this is a risk that I choose to take in order to avoid log in every time. I feel that I have good enough control over my things.”

Computers and mobile phones are different in screen size, capacity and the way you interact with them, however do we separate between the type of information we store on the phone compared with what we would store on a computer?

- “There is in general more information on the computer; the content on my phone is like a small section of the content on the computer.”
- “There are some things I only have access to on my phone, like applications. But I try to synchronize as much content as possible, so that I can access the information both from my phone and computer. Initially mail and calendar.”
- “If I had some really sensitive and personal information I’d rather store it on my PC than the phone”
- “I don’t think there are things that I would only store on my phone.”

One informant expressed that the computer is safer than the phone because “It is always with you, while the PC is not”. Referring to how easy it is to lose a phone. Another student did not separate the security level on the phone and the computer that much.

- “The only way the computer is more secure than the phone is that I don’t risk losing the computer. I can’t get my computer stolen in town.”

Some interviewees had more technical insight that was crucial to their perception of security.

- “If I had a code on both my phone and my computer I would probably feel that my phone is safer because one can always just remove the hard disk to get access to the information unless it’s been encrypted.”
- “I can encrypt the file system on my Mac, it’s quite easy, but if I then forget the password there I’m in trouble. It will probably not happen, but it is just so boring if I

do.”

- “I don’t think either one is more secure. If you want to unlock a phone it’s only four digits (iPhone) while on the computer you have more opportunities and can create a safer password. However I guess you can only Google how you crack a password in a computer, but it’s not the same for phones.”

On the question if there were any information that they would only store on either the computer or the mobile the students agreed that they would not store personal information, like high quality pictures taken with a camera or a hospital journal, because it is more likely that the phone is stolen. However it was also pointed out that she believed that if it got into the wrong hands it would be just as easy to get information from a phone as from a computer.

All of the informants would feel that it was worse to lose their computer, then their phone, because of the amount of data is larger. The information on the phone is more or less also available on the computer, which makes it a smaller loss.

5.2.3 Probe responses

Students both with and without screen lock on their phones were interviewed and asked about why they had chosen one or the other. The two groups had valued different things. The students with activated screen lock were more concerned about security, and experienced that the need for a screen lock increases in line with the amount of content on the phone.

- “Didn’t have a screen lock, but now I keep data for my master on my phone and have to protect it.”

The students without a screen lock were more concerned about the time, and experienced a screen lock as a stress factor. “(...) I want to have instant access to my applications when I’m going to use them.”

On the question of how the students thought about lending their phone away to friends they answered that they had no problem with that, but would like to know their agenda and prefer not to lend it out for too long. They experience the content on their phone as quite private “Everything on it represents me and my interests.” However some things are more private than others

- “I have no problem lending out my phone, but would have liked a lock on my images and notes for instance. If that existed the threshold for lending it to others would have been lower. I have seen something like it on App Store, but it could only contain ten images.”

5.2.4 The cloud

The cloud is a metaphor for the Internet, talking about the cloud in this setting includes services like Dropbox that allows you to save and access files online. This part of the interview was suppose to give an impression of how people relate to the cloud and the security around it.

All of the students were familiar with the term *the cloud* and were active users of cloud based services. However they grade the cloud as less secure than a computer, and there are still some types of content that they were not comfortable with saving in the cloud.

- “If it was a very sensitive file I would probably not have saved it in the cloud.”
- “You feel that you are on a web page, logging into something that is not yours.”
- “I don’t feel that it is the authentication that is unsafe, it’s like locking up a door to a room with no walls. Where strangers, the owners or hackers, can just walk right in without a key. I have little confidence in the internet.”
- “I feel like I have more control over files saved on my own computer, but I don’t think much about it. However there are some things I feel that are safer to save on the web, for instance Dropbox, if the computer crashes or it was a fire.”

In spite of the skepticism of the cloud services all of the students were users of Dropbox or similar services. When it comes to the question of the rights-holders of the content stored on the web, the students had no or little knowledge about this., and had not read the user agreements.

- “Well, yes I think about it, but try not to, if you are going to use the service, you just have to accept the user agreement.”
- “I try to use services that have many users, if something happened the media would catch it, and I would be informed.”

Most of the interviews uncovered that the students tend to reuse passwords across services, but one interviewee were using several different passwords.

- “If it is something less important I chose a simpler password that are easier to remember, but I also have more advanced passwords on things I’d like to protect more, like mail.”

5.2.5 Probe responses

In order to better understand the results from the probes I presented some of them to the informants and asked the them to comment on the outcome. There were different explanations of why people don’t have a screen lock.

- “I have the opportunity to remotely turn on the screen lock, so I feel that if I my phone was taken I would have the opportunity to do something. I would have felt less secure if that wasn’t possible, and probably have activated the screen lock”
- “I have my phone with me all the time, in my pocket or right next to me, I have control of were it is, so why should I’ve had a pin-code or pattern(..) It would have been better if I just could have used my thumb”
- “I’m thinking people just don’t bother, or don’t prioritize it.”

5 Findings

- “I’m thinking that it’s because people feel that it is cumbersome since you actively have to turn it on.”

The students rated their experience of security of the content on their phones as medium secure. Again this was explained with the fact that people feel that they have control over their phones and therefore also over the content even without a screen lock. Another person states that we probably don’t know enough about the technology since it’s just a feeling “I feel that my information is safe, but I don’t know if it is!” It seems that people have relatively little confidence in the screen lock. “Nothing is secure, everything can be hacked” but they don’t believe that their phone will be of particular interest to strangers. “Why would anyone be interested in the content on my phone anyway?”

Some of the images taken by the participants of the probes were presented to facilitate a discussion of how context affect how people use their phone. The images displayed different situations and location; at home, at school, in the retail store, at a football stadium, at a café, on the subway, on a party and outside in the streets.

- “If I’m in the store and have to check my my mobile bank application, I hold the phone close and make sure that there are no people around me because I don’t want anyone to see my identity number.”
- Are there anything you would not login to if you were at a football stadium? “No, I think I could have logged into everything, I’d just look a little bit extra over my shoulder first”
- “I have some apps that I think is a bit embarrassing to use in social settings”
- “One time on a field trip I were filling up my prepaid phone by entering a number in a text. However before I was finished, the guy in the buss seat behind me had copied the number and used it to fill up his phone. I got the money back later, but these things can happen!”
- “If I’m typing in a password on the subway or something I make sure people cannot see it. That’s the biggest difference”
- In a social setting like on a party: “If I know that only I can see then I could have logged into almost anything, but I would probably not have visited my mobile banking application since people could just turn their head and see it.”

Next we compared the password and pattern graphs of how secure these different authentication mechanisms are experienced by the students. As the graph showed the interviews also confirmed that the general opinion was that patterns as authentication was less secure then the password. They stated that that password can be as easy to remember as a pattern, but for a stranger it’s easier to get hold of a pattern, as it is being displayed on the screen it is easier to copy.

- “If my phone was stolen I would have been less worried if I had a screen lock then if I

didn't.”

- “Password is a method that you are more familiar with, and feel a bit safer because of that”
- “To draw a pattern seems very simple”

At the end of the interview the student got the opportunity to chose a preferred authentication mechanisms between two options presented with and without a password meter measuring the strength. The point of this was to see if a visualization of the security level affected the users choice. First normal password and a Windows 8 pattern.

- “I would have preferred the password, more logic, what I'm used to.”
- A person without a screen lock answered: “I would have chosen the pattern, but if I went for the password I would probably have used one I had from before. The pattern is easier to press on a phone, a keyboard is different from a computer to a phone, so I'm thinking that pattern would fit the screen on a phone better than a keyboard does. Some passwords have special characters or a combination of capital and regular letters, which is what a good password should have, but this takes very long to type in.”
- “I think I would have chosen the password. It's the standard and what I'm most used to.”
- “For simplicity's sake I would have chosen the pattern, but for safety's sake I'd go for the password, as long as it's a password that I know is good and hard to crack.”

Password meters are measuring the security of the password and gives a visual representation of it back to the user. However the interviews revealed that the password meters don't have a very big influence on what authentication mechanisms these students choses. They trust their own ability to create safe passwords more than the password meters, and would rather use an authentication mechanisms they are familiar with than a new one, even though the password meter says it's less secure.

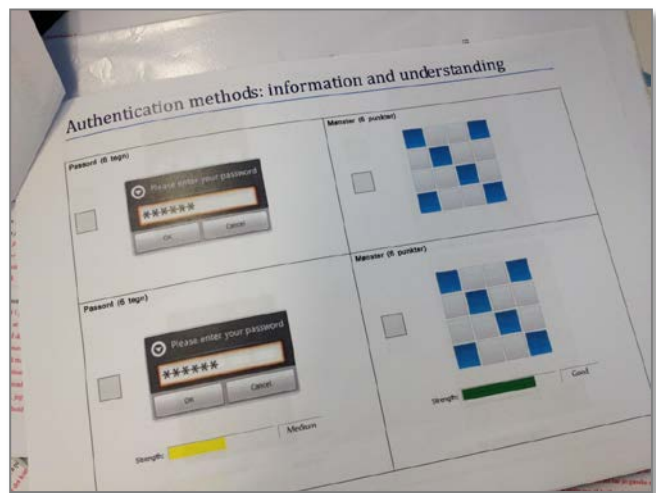


Figure 5.5 Password vs. Pattern

- “Well often I don't completely trust those (..) If it was a really big difference, if one was really bad while the other was really good maybe, but when they are so similar that I would have stuck to the password.”
- “Sometimes they doesn't match reality”

5 Findings

- “There are so many different indicators, you can type in a password in one and get a good security and type the same password in another one and there it’s bad, it depends on what dictionary it uses.”

The E-Me project have created a set of different authentication mechanisms and tested them out on older people. One of these alternative mechanisms was recognition of images and sounds. I changed the layout of the interface in order to make it look more like a mobile interface and put it up against the pin-code authentication. None of the interviewees had seen anything like that before, and had to be explained the idea behind it.

- “It would be much easier to remember then the pattern at least, because here you can associate to the images to things, make a story or something like that.”
- “I would have gone for the pin, but that’s just because that one (with images) looks a bit weird. But I feel that they are very similar in relation to security”
- “I would have chosen that one (with images), because it’s the coolest. It’s more entertaining.” Would you have felt it was as secure as the pin-code? ”Yes I would, and maybe even more secure if the pictures were placed in a random order.”
- “I don’t look at it as more stress selecting four images then typing four numbers, it’s the same principle, four numbers, four images, it’s exactly the same”
- “It does not matter which one I use. That one looks a bit childish with the pictures and all that, but if it looked more stylish, or had other pictures then a pig and a sheep and so (..) I like it, but the reason I would still chose the pin-code is that I don’t think it look good, if I get two alternatives I’ll take the one that looks nicer”

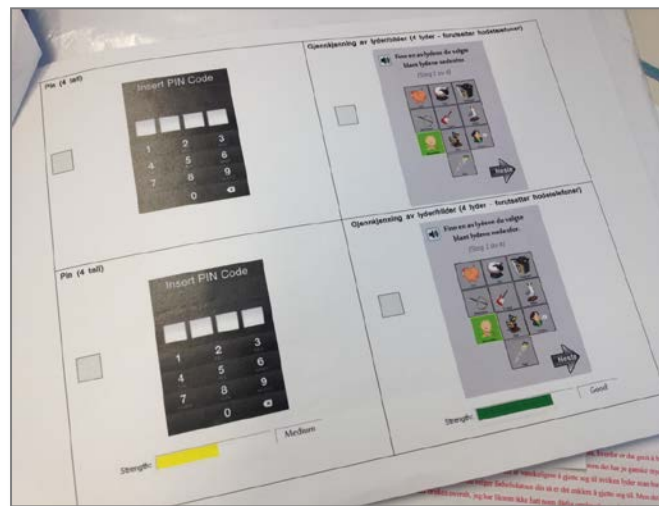


Figure 5.6 PIN-code vs. Images

Displaying password meters did not make any difference to the students choice this time either, and all of the students confirmed that they would not change their choice because of

them. Some feels that they are more annoying then helping.

- About the pin-code: "It's what I'm used to, and it's difficult to guess (...), I believe it's harder to guess which sounds one have chosen then which numbers (...) But pin is used everywhere, and I have not had any bad experiences with the pin-code."
- "I only think it's really annoying such password meters appear, because suddenly I have to change my password, use a capital letter for instance."

5.3 Eye tracking

The eye tracking were conducted with five people, the first one as a pilot study. The informants went through two different tasks. First they used the Feide authentication to login to Vortex⁵ and second they went through a prototype developed by the e-Me project. The tracking were conducted on the students own phones, and the software was recalibrated for each person. The informants were informed that they could rotate the phone 90 degrees if they preferred the screen to be horizontal.

There were generated a lot of data from the testing, but with only valid results from four uses, it was more appropriate to use gaze plots then a heat map. In the gaze plots each color represent different participants. Even if all of the results are displayed with an iPhone in the background the orange participant was using an Android phone.

5.3.1 Feide

Feide does provide documentation for developers that want to include Feide login in their applications. The case that was used in this task was however accessing a university service through a normal website in a mobile browser and not an through an application. As mentioned Feide was not adapted to the mobile screen, which was noticed because some of the text overlapped and the content was too wide, so in addition to scrolling up and down the users had to scroll left and right to see everything. The small text did also make it difficult to read without zoom.

The Feide login process consisted of four steps for the user:

1. Select Feide on UiOs site
2. Select affiliation
3. Type in username and password.
4. Accept the information that will be sent to Vortex (adm.uio.no)

People have different passwords and usernames with different characters and lengths, so comparing the gaze plot from different people would not necessary generate useful data (see

⁵

<http://www.uio.no/tjenester/it/web/vortex/>

5 Findings

figure 5.7). Some users have difficulties typing on the touch screen and it was confirmed during the testing was that typing on a touch screen can be a difficult. Several of the users had to type in their information more than one time because of typos.

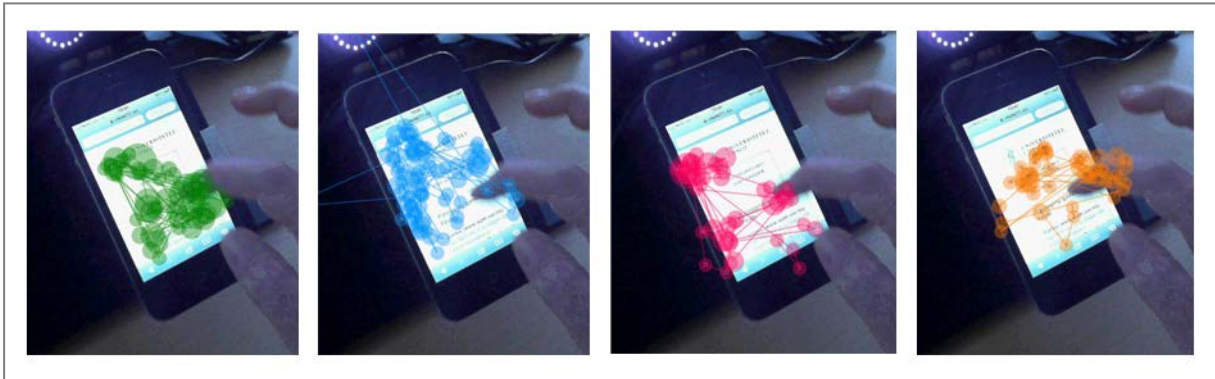


Figure 5.7 Type username and password

Log-in with Feide involves more than just typing in password and username. In figure 5.8 we can see a gaze plot from the step where four students choose the University of Oslo as affiliation. The pink gaze plot is unfortunately slightly shifted relative to the background. But we can see that all of the students follow a similar pattern. They look more to the left of the screen with most focus on in the middle, when they look at the drop down list. This is natural as we in Norway reads from left to right.

In addition to some usability issues because the service is just not adapted to mobile, the informants met other unexpected challenges. Even though they accessed the service from www.uio.no they still had to choose the University of Oslo as affiliation. The list of affiliations did however follow the standards of iPhone and Android. A list with radio buttons on Android and a spinner on iPhone.

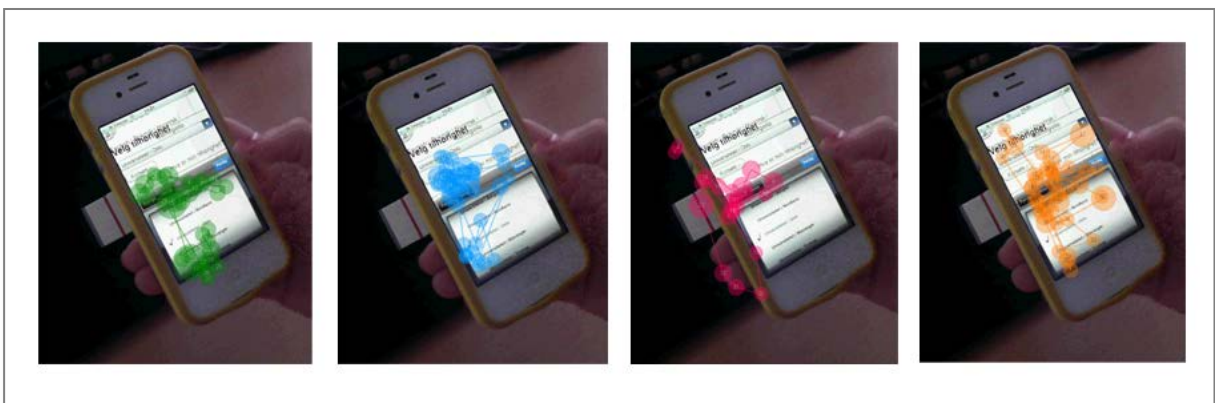


Figure 5.8 Chose affiliation

In figure 5.9 the gaze plots displays how the students look at the information about them that are shared with the affiliation. The users skimmed through the information text but did not completely understand all of it. One user chose for instance to press the button “do not

accept”, on the last step, which meant that she had to go back and log in again. This was explained with insecurity of what the information would be used for and where it was sent. From the gaze plot (orange) it was possible to see that the student did not read the text carefully before this decision was made. Another user pointed out that the information that would be sent to Vortex was incomprehensible and looked like code. This student (pink), in contrast to the orange user, according to the gaze plot, looked more closely on the page.

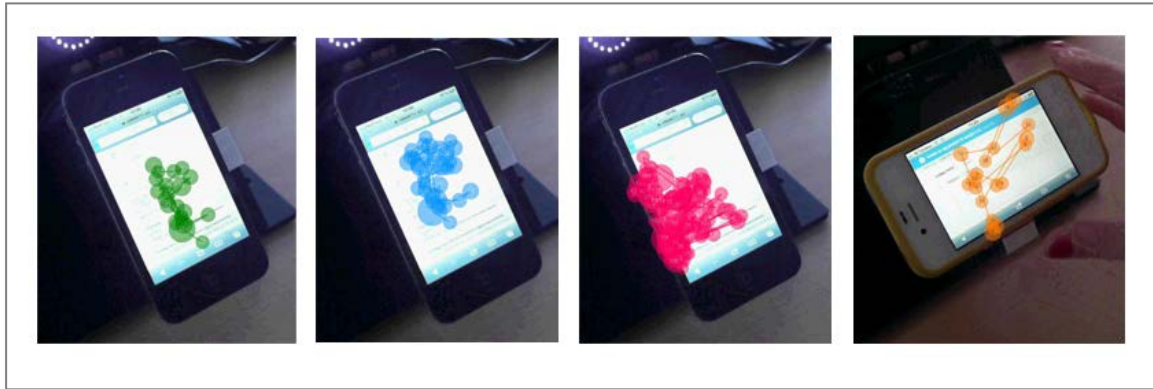


Figure 5.9 Read and accept conditions

One of the questions that the informants were asked were their knowledge of Feide as a login service. Several mentioned that they had used it before on other University services like the library page Bibsys. They were also asked if they felt that it was a safe method to use, whereas they replied “Since we’re accessing Feide through the University pages I guess it is safe” and “I guess it is as safe as other login methods”. From the questions that were asked after the testing it was clear that some of the informants were not familiar with Vortex either.

5.3.2 e-Me

In this section only some of the findings will be presented, while a more complete set of findings from the eye tracking of the e-Me prototype is available in Appendix H. As a step in the process of finding out what authentication mechanism that works best on touch phones gaze plots from different methods are compared.



Figure 5.10 Images vs. Pattern

5 Findings

Here are some gaze plots from the testing. Figure 5.10 displays the eye movements from one user during the image and pattern authentication. Opposed to the pattern authentication the image authentication has four steps, and the eye movement throughout all the four steps was captured. As one can see the gaze moves much more on the image authentication, and are also more spread, then on the pattern authentication.



Figure 5.11 Password vs. Pattern

When comparing password and pattern authentication in figure 5.11 we see some of the same tendencies as on figure 5.12. The gaze is spread almost all over the screen. When typing in user name and password the gaze switches its focus between the keyboard and the text field.

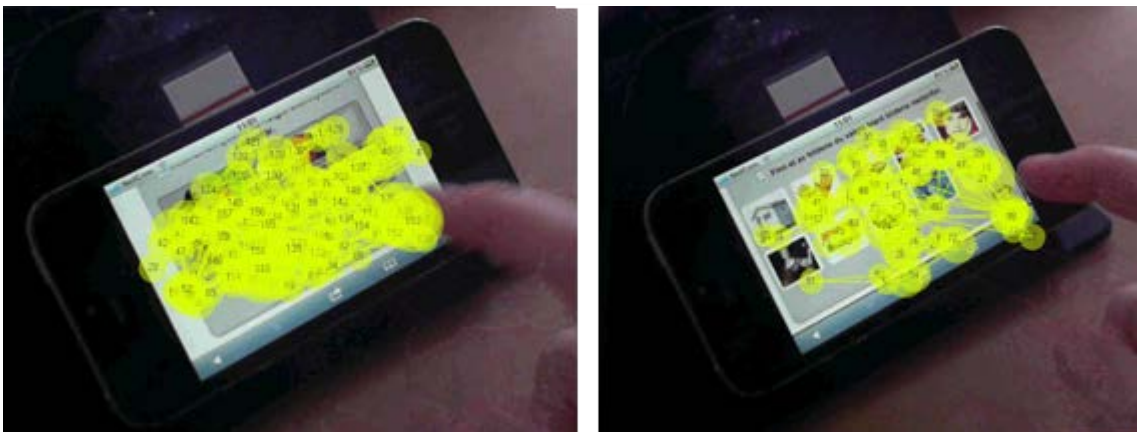


Figure 5.12 Sound vs. Images

The sounds did not work in any of the phones because it depended on Java Script, but the students still had to go through and complete this step to get to the next one. Due to this the authentication became very similar to the image authentication, the main difference was that the images were labeled and had gray background instead of white. On the gaze plot in figure 7 we can see that the students gaze are moving more on the sound authentication then on the image authentication.

5 Findings

At the end of the session the students were asked to assess the five different alternatives based on how well they liked them with numbers 1-5. 1 = very poor, 2 = poor, 3 = medium, 4 = good, 5, very good. From their comments during the testing and the evaluation it appears that they emphasized factors like; easy to remember, secure, nice to look at, fast and easy to use.

5.2 Evaluation of authentication mechanisms

	Password	Questions	Sounds	Images	Pattern
Student 1	5	2	2	2	4
Student 2	3	2	3	4	3
Student 3	4	1	3	3	2
Student 4	5	2	1	1	3
Student 5	4	1	0	5	4
Total	21	9	9	15	16

From these numbers the password authentication clearly stands out from the others with a much higher total number. The question authentication was one of the mechanisms that was least liked by the students. They commented that it was cumbersome to set up and that they did not experience it as a very secure mechanism. As the sounds did not work and the students were told to just treat it as it was only images, the evaluation of this method is not counted as valid.

The image authentication got 15 points. This method was new to all of the users and some were unsure if they would be able to remember the combination of images and one commented that the images were too alike. In spite of this they all managed to complete the authentication. The pattern consisted of 5x5 squares where the user should pick a pattern with 6 squares. This method is quite similar to the pattern available on Android phones except that the finger is not dragged between the selected points.

Looking beyond the total number and instead how each student has evaluated the methods one can see that they do not agree very much in their assessments. The image authentication for instance is given points all the way across the range from 1 to 5.

The informants commented that images could be hard to remember because they had no personal attachment to the specific images. A student would have liked to pick out her own images. On the other hand we have the password which is custom made, something people can relate to and therefore are easier to remember. Questions could be custom made, but also selected from a list, most of the questions in the list asked about personal matters, like what's the name of your grand dad. The answers to that kind of personal questions are not too hard to figure out if you know the person, especially not when you also can add hints. So this type of

5 Findings

authentication could be easy to remember, but are not experienced as secure enough by the users.

The users are quite attached to the password authentication which is the one they are used to, and were negative about getting another authentication ID they have to remember in addition to the one they already have.

6 Discussion



Figure 6.1 Dilbert by Scott Adams (2007-11-16)

Several methods have been applied in order to increase the reliability of this study. The methods complement each other and are intended to enable the research questions to be answered in the best possible way. In this chapter the findings from the different methods will be discussed with the theoretical aspects that have been described earlier as a basis.

6.1 Review of authentication mechanisms on touch phones



Make a review of authentication mechanisms on touch phones.

In this section research question one will be discussed. The research done in this project shows that most applications are normally only logged into once, and never logged out of. The users only use the back/home button to get out of it. This means that most applications are open and available for everyone who can access the phone. The screen lock have become, in many cases the only protection to the content on the phone, it has almost the same function as a single sign-on (SSO) and a very important role as the only security protection (30).

With Android phones we are introduced to the pattern screen lock, but the general perception among the informants seems to be that the password or the pin are more secure options. The users are familiar with passwords from stationary terminals and desktop services, and have used it for many years, while the pattern was introduced only a couple of years ago together with the touch phone. The users have had less time to get to know this mechanism.

We already know that typing on touch phones can be cumbersome. Password authentication is something that have been transferred from the web and were initially intended to be used in combination with an external keyboard. One could ask; what if the touch screen was invented first, would other types of authentication mechanisms have taken the password position?

Table 2.3 presents several screen locks where a diversity of interaction methods have been adopted and put into use. These authentication mechanisms will be reviewed based on W3Cs recommendations for user input in Mobile Best Practices 1.0 (26), and the concepts of direct manipulation and context as these are among the things that separates authentication on touch phones from stationary terminals with GIMP interface. Last they I have looked at the quality of the screen locks when it comes to efficiency and if they are easy to remember, which were some of the features that the informants meant was important for authentication mechanisms.

6.1 Review of authentication mechanisms

	Minimal keystrokes?	No free text entry?	Specified default entry mode/ input format?	Secure in all context?	Efficient?	Easy to remember?
Password	?	✓	✓	✓	/	?
PIN-code	✓	✓	✓	/	✓	✓
Pattern	?	✓	✓	/	?	?
Slider	✓	✓	✓	/	✓	✓
Circle	✓	✓	✓	/	✓	✓
Biometric	✓	✓	✓	?	✓	?
Piano	?	✓	✓	/	?	?
Picture gesture	?	✓	✓	/	?	?
Bluetooth	✓	✓	✓	✓	✓	✓
NFC	✓	✓	✓	✓	✓	✓
✓ Meet the requirement. / No ? Depends (e.g. length/sound/complexity)						

The Mobile Best Practices 1.0 says that one should keep the number of keystroke to a minimum, this is understandable as text input on touch phones can be cumbersome. One reason that it is cumbersome to write on touch phones is that the keys on the keyboard are very small and there are little or no haptic affordance of feedback. This means that the users must look at the screen while typing to hit the correct buttons. People with larger fingers will experience more problems then people with small fingers.

Krug states in his second law that the number of keystrokes actually don't have anything to say, as long as they are mindless and unambiguous to perform(15). The *password* mechanism was rated high among the students, the informants commented that it feels safe, they are more logic, and what they are used to. When they tested the Feide login on their touch phone several users had to retype the password because of typos, but the password was still the most

preferred mechanism. Users have no problems remembering passwords they use often, on stationary terminals they type in the password without thinking or counting clicks. The informants confirmed that they preferred to type on a PC rather than a touch screen.

When it comes to efficiency the small keys kept the error rate high and some users experienced that it could be difficult to complete the password authentication fast. Looking at the other mechanisms we can see that the pin-code have a limit of four numbers, and the keys are also larger than on the QWERTY key pad. This makes it both physically easier to type and more efficient as the error rate probably are lower. The pattern, the piano application and the picture gestures does also have larger areas to interact with, there are more possible combinations, but because it would be easier to hit the correct button it would probably also be more efficient than the password.

On authentication mechanisms there are no room for free text entry as the mechanism only accept user input that matches the combination that were created when the it was activated. The input format is predefined, for instance can the user not type in anything other than numbers in the PIN-code, and if a NFC screen lock were activated it would not be possible to unlock the phone with a Bluetooth device. Therefore the users don't need to think and make a choice, which probably would extend the time it took to login.

Gestural interfaces and direct manipulation are no longer only desktop metaphors and joystick(18). Direct manipulation on touch phones involves manipulating objects with touch gestures on the screen. I would separate the password and PIN-code from for instance the pattern, piano and picture gesture. Typing in a password the user focus on the keyboard while the letters appear in a text field above, when drawing a pattern the interaction is more similar to actually draw on a piece of paper rather than draw in Paint on a PC. The advantage with these mechanisms is that they are based on natural gestures which are easy to learn as the interaction is similar to how humans interact with physical objects (18). The disadvantage with gestural interfaces is that gestures often are visible by others and in an authentication process this can affect the privacy of the user (18). Large buttons might be easier to hit, but would also be easier visible by others. The authentication mechanisms that are based on direct manipulation and natural gestures, the pattern, slider, circle, piano and picture gestures would therefore probably be less secure in crowded contexts. While the password have small keys and hidden characters, which would make it more difficult to see and copy, by unauthorized people.

From the findings it is clear that students wants the authentication mechanism on their touch phone to be easy to remember and efficient to use. When a previous version of the e-Me prototype were tested on elderly, they also pointed out that their password had to be "easy to remember". According to Sharp, Rogers and Preece (13) the requirement for people to remember and recall a lot of information will put a big memory load on the user. As we've learned from the findings, and also stated by Don Norman(24), reuse and short and simple passwords are the way people minimize their memory load. This does affect the security of the service, but there are measures that can be implemented to avoid people taking short cuts.

By emphasizing recognition rather than recall, making objects, actions, and options visible the users memory load would be minimized (13). This is what was done in the e-Me prototype, where images and sound was used for authentication. During the user testing the informants expressed their uncertainty in relation to these mechanisms, if they would be able to remember it, however all of them managed to get the combination right on the first try. The advantage were that they actually didn't have to remember the combination, only recognize the images when they saw them.

Password, pin-code, pattern, voice recognition, piano, and picture gesture are all mechanisms that are depending on the users memory, *something the user know* (37). This is the most common way to authenticate humans (37). Fingerprint and face recognition are biometric methods requiring *something you are*, while proximity-based and NFC requires *something you have*. The advantage with security tokens like the NFC and proximity-based authentication is that it would not require direct input from the user or the user to remember any specific information, as the phone would be unlocked by sensors in the phone communicating with the token. The disadvantage is that there is always a risk that such tokens can be stolen or lost, and this risk would naturally increase in a public or crowded context.

Voice recognition require both something the user know and something the user are, and according to Schneiders theory (37) it should therefore be safer then the others mechanisms. Looking at voice recognition from a mobile perspective this might not be the best option due to the varying context of use. Talking loud to your phone is not always appropriate and the users would probably be hesitant of doing so in a public context. It can almost be compared to saying your password out loud, which is something most people would not do. Schneiders is right when he states that all types of authentications rely on something you know, something you have, something you are or a combinations of these, but on mobile devices the context also have to be taken into consideration when determine what is a good and less good mechanisms.

6.1.1 Risk and security

The risk level on a touch phone will vary a lot, there are several factors deciding the risk level. First and foremost the content on the phone is critical. What type of applications there are on a phone, and how many applications with critical content. In order to decide which risk level that would be appropriate on a phone one could look at table 6.2 that are describing four different levels. The statements that most likely could be applicable to touch phones are marked with a frame.

6 Discussion

6.2 Risk Levels (29)

	Risk level 1 None	Risk level 2 Small	Risk level 3 Moderate	Risk level 4 Large
Consequences for health and life	There are no danger of loss of life and / or human health.	There can be small injuries	There can be moderate injuries	There may be loss of life and / or public health
Economic loss/ more work/ increased costs.	No economic loss/ more work/ increased costs	It can lead to small economic loss / additional work / increased costs	Violations can result in moderate financial loss / additional work / increased costs	Violations can result in large financial loss / additional work / increased costs
Loss of reputation (reputation, trust and integrity)	No damage to reputation.	Any damage to reputation is considered to be small.	Reputation may be somewhat impaired in a shorter period of time.	Reputation may be impaired for a long time, eventually lasting.
Obstacle in criminal prosecution	No contribution to the prevention of criminal prosecution.	Minimal contribution to the prevention of criminal prosecution.	Moderate contribution to the prevention of criminal prosecution.	There may be obstacles in the prosecution.
Negligent contribution to the offense	It can not be negligent assistance to crime.	It can not be negligent assistance to crime.	It can not be negligent assistance to crime.	Violations may contribute to negligent assistance to crime.
Inconvenience / disadvantages	No nuisance or inconvenience.	There can be some inconvenience or hassle.	Not relevant.	Not relevant.

Normally, losing a phone do no have any direct impact on the users life and health. There are few applications today containing detailed health information and web sites can be accessed from other devices. As for economical aspects there can be moderate financial loss, this can be caused by for instance international phone calls, which one of the informants had experiences, or downloading of applications etc. If unauthorized people get access to the mail account or social media accounts they can harm the owners reputation by performing offensive actions in the owners name. There are several stories where people have gained access to the phone of a celebrity and spread private pictures on the web, depending on what type of pictures it is, this can of course harm their reputation and it is certainly an inconvenience to the owner. In addition to offensive behavior ID theft can also work as an contribute in to violate the law, but probably not to a large extent.

There is never a good time for loosing your phone or authorization to it. According to the interviewees there are several measures they would take if they were suspecting that

unauthorized people had gained access to their phone. For instance changing all passwords and remotely deleting the content. This options does improve the security, but it is still inconvenient for the one that have to do it.

The majority of the screen locks mentioned above does not qualify for any higher security level then level 1 according to table 2.2. How it works today is that all solutions that do not satisfy the demands for security level 2 will be classified in level 1. Security level 1 includes self-defined passwords and usernames on the web, and all of the authorization mechanisms would have to be self-defined on the phone. The exception is proximity-based and near field communication mechanisms that are depending on a security token in addition to a phone, which could qualify as security level 2.

When deciding on which security level that would be appropriate for a mobile device one should also take the context of use into consideration as well as the risk level. Because the context of use varies the need for security also varies. In a crowded bar there will most likely be a greater need for a screen lock then at home in your own living room. Flng (16) talks about context with a capital C and a lower case c, describing that there are different situations and there are different locations. The need for security in one location can change based on the situation. If you are home alone in your apartment the need for security will probably be smaller then if you are throwing a huge party with a lot of strangers. This is one of the reasons why location based authentication in many cases would not be appropriate.

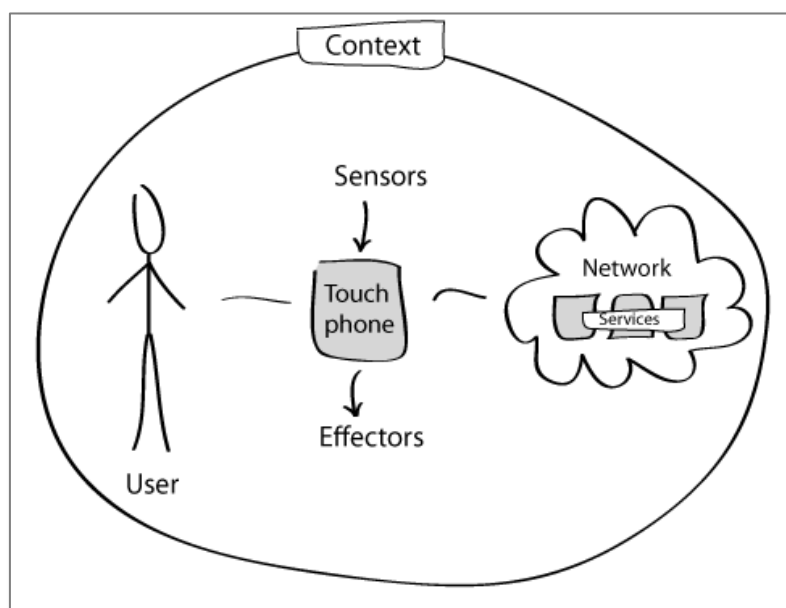


Figure 6.2 The ecology of the touch phone

To understand the difference between touch phones and stationary terminals and their context, it is appropriate to go back to the ecology of devices. The touch phone receive input from several sensors, some sensors are retrieving input directly from the environment, like gyro, accelerometer, GPS and camera. Other input comes directly from the users, through touch interaction and speech. Effectors on the other hand gives feedback to the users in form of

sound, light and vibrations. Stationary terminals do have a lot of the same sensors, but the main difference is that the sensors who retrieve input from the surroundings through movement are not present. The input that touch phones can receive and the source it is received from varies a lot, which means that there are more factors that have to be considered when talking about security.

Computer scientist Butler Lampson (14) suggests to use two separate machines to reconcile accountability with the freedom that internet enables. A *green* terminal that demands accountability, for more important things like personal information, work data and backups, and a *red* terminal that does not demand accountability in the same degree, where one can store content that one are not too concerned about losing. Not that many have several PC's, but lots of people does have both a PC and a touch phone or other devices.

From the interviews we've learned that the students uses their phone to access basically the same information as they do with their PC. If it was a question of what they would prefer to lose, they all chose the phone. This had a lot to do with the price, but also the content they would lose. The computer were used for backups and saving large data files like school papers and high quality images. Phones are often synchronized with a PC and therefore become a section of the PC and most things on the phone would also be available there. A students mentioned that "loosing the pictures on the phone would be sad, but it is worse to to lose the high quality images on the computer."

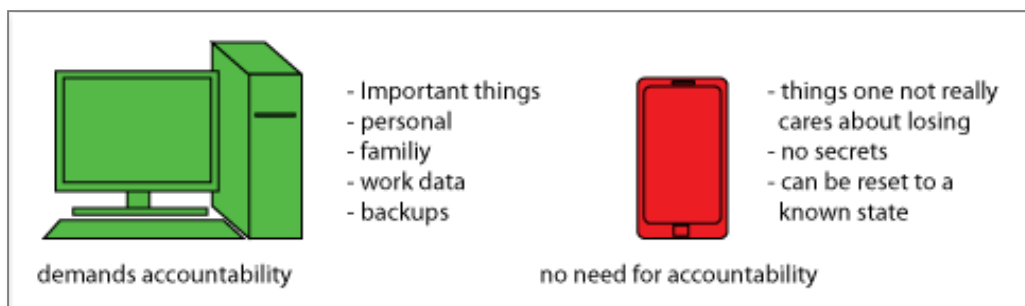


Figure 6.3 green and red terminals

Lampson's division sounds sensible, but the reality today makes it more complex. More and more information are stored on the web, and can be accessed from all devices connected to the internet, services like work mail or internet banking. This makes it almost impossible to completely separate data that demands accountability and data that doesn't. Devices and computers are now basically just different doors giving access to the same data (the cloud) in different ways. Because most applications on our touch phones are only logged into once and are constantly running, a touch phone without a screen lock is like an open door to the cloud.

According to Thorsheim (69) sensitive data should not be saved on mobile phones. The reality today is that a four digit pin-code will take an hour to crack, maximum. However a password of six characters, containing both numbers and letters will constitute a password that is much harder to crack. The reason that he does not propose a longer password is that typing long

passwords can be challenging, especially on touch devices. Thorsheim also points out that security must be linked to usability for it to act in the best possible way (69).

6.1.2 Security and usability

Like the graph in figure 6.4 visualizes it is an issue that as a system gets more secure, it also becomes less usable. Security features can be clumsy and awkward and can present significant obstacles of getting work done. As a result of this, security measures are all too often disabled or bypassed by the users they are intended to protect (14). Don Norman have commented that “the more secure a system, the less secure a system”- if the users find that the security gets in their way, they figure out way to bypass it. This is what happens with the screen lock on mobile phones. The users finds that the screen lock is standing in their way of performing their desired actions efficiently enough, and therefore disables it. This way the user, knowingly or unknowingly compromise the security of computer systems or contribute to the unwanted release of personal of other confidential information.

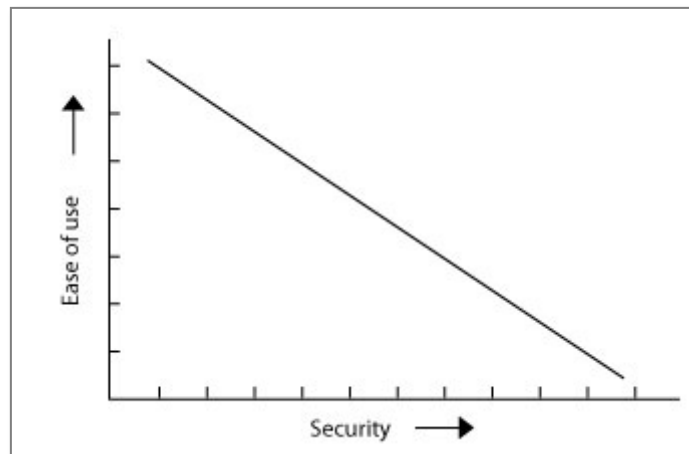


Figure 6.4 The relationship between usability and security

When using screen locks or password and username to protect information, it is to protect it from threats in the environment. Threats might be other human beings, a natural phenomenon or another computer system etc. The threats launch an attack towards the system, and will be successful if it can exploit vulnerability in the system and do an intrusion (70). In a mobile context the system are exposed to additional threats then the ones that are present on stationary devices. Using the phone in public places like the subway, or at a party the surroundings are less predictable then in an office or home. Users connect to unknown and unsecure wireless networks and it is more difficult to control who sees the screen on your device.

The authentication security is only as good as the weakest link in the chain (36), and the weakest link is often the user. Because the users are afraid to forget the password or think it is stress to type, they tend to chose simple passwords, passwords that they use on many other services or no passwords at all.

More and more sensitive information will be stored in systems whose security does not

necessarily increase in proportion to the value of the assets they contain, like the touch phone. New vulnerabilities will emerge as previously unknown weaknesses are uncovered and as innovation leads to the use of IT in new applications and the deployment of new technologies. The growing complexity of IT systems and the fast-growing importance of network access and network-intermediate computing are likely to increase the emergence of new vulnerabilities (14).

Don Norman (14) states that more security does not necessarily needs to make things complex or less attractive to use. It looks like the graph is still applicable based on the screen locks that were reviewed. Because of the challenges users experience with writing on a touch screen exploring other types of input is relevant. One approach to reduce the number of keystrokes is to rely on recognition rather than recall, this will also keep the users memory load to a minimum. Not many authentication mechanisms are following this principle, possibly because it is not much documentation on this type of authentication mechanisms, and that the level of security is experienced as lower. It is therefor possible that there are a lot of undiscovered opportunities with this type of authentication.

6.2 Mental Model of Security



Examine the term mental model of security. How can we utilize the concept of mental models in design of authentication mechanisms for touch phones?

In this section I will, according to research question two, investigate the term mental model of security in connection with touch phones and stationary terminals, and discuss how information about peoples mental model can help designers to improve their products.

6.2.1 What is the users mental model of security?

A users mental model is based on personal preferences like previous experience and knowledge. Susan Carey (71) defined the term mental model in a journal article, Cognitive science and science education, from 1986:

“A mental model represents a person’s thought process for how something works (i.e., a person’s understanding of the surrounding world). Mental models are based on incomplete facts, past experiences, and even intuitive perceptions. They help shape actions and behavior, influence what people pay attention to in complicated situations, and define how people approach and solve problems.”

Most of todays generation of students used feature phones (16) before they switched to touch phones. Their mental model is therefore colored by their experience from feature phones, which were basically only used for texting, calling, and maybe listen to music and play simple games. With touch phones a new way of thinking appeared. From buying a phone with a fixed set of features the touch phones enabled users to decide the content themselves by

downloading applications. Using applications is something most people are familiar with from laptops and stationary terminals. In addition to the obvious relation to feature phones, the touch phone also have a lot of the same features and qualities as a PC.

The users' initial mental model of the touch phone are influenced by their past experience. For most people this will probably be a combination of the mental model of the stationary terminal and the feature phone. Assumptions, norms, and expectations may change over time (14), and the mental model does also evolve as the user get more experienced (7). When people buy their second touch phone they are more experienced, and their mental model will be more based on their experience from the last touch phone they owned.

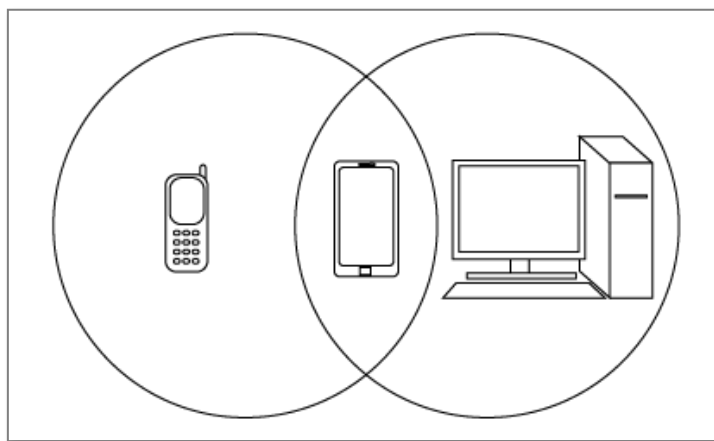


Figure 6.5 The mental model of a touch phone

6.2.2 How can we take advantage of mental models in design?

In this thesis peoples mental model of security have been investigated by listening to the users, learn about their past experience, observing their behavior and through interviews getting to know how they think regarding security and authentication mechanisms. Based on Careys definition I would describe a users mental model of security as the person's thought process of the risk level and what security measures that should be implemented in order to maintain a low risk. While a users mental model of security mechanisms on the other hand could be described as a persons expectations and understanding of the mechanism, how the interaction works and how well it can protect the content. I will first talk about mental model of security in general.

Lampson (14) states that security on laptops and stationary terminals are in bad shape, people worry about it a lot and spend much money on it, but most systems are insecure. The primary reason for this is, according to Lampson, that users does not have a model of security that they can understand. All trust is local and people chose for them selves who and what to trust or not to trust. In order to improve users understanding simple models of security are needed (14). Touch phones have been a public domain since about 2007, because of the rapid development within the world of technology this is a long time, but compared to the existence of the stationary terminals and laptops the touch phone is still young. This is the basis for exploring the assumption that there also are room for improving peoples mental model for

security on touch phones.

The students that were interviewed could be divided into two groups. Students with and without a screen lock on their touch phone. The trend seemed to be that persons with screen lock were more skeptical about saving passwords and usernames in their desktop browser, while persons where the screen lock not were activated more often said yes to save their password and username in the browser. All of the students knew their phone potentially were exposed to a greater risk, but not unexpectedly some were more concerned about security then others.

Several of the informants were using bank applications, which requires authentication every time they use it. The reason why this were accepted by the users were that they classified it as a big threat if this content were exposed to strangers and would not even have considered keeping this application unlocked. Loosing money is something we are familiar with, there have always been pickpockets and we have always taken care of our wallets and credit cards in order to avoid them. If unauthorized people get access to a touch phone, loosing money is not peoples biggest concern. The students were more afraid that someone would abuse their e-mail or their Facebook account and damage their reputation. Identity theft is a crime that has not really been a major problem until the computer became common, and even though there have been more focus on it the last years, it is probably difficult for most to relate to.

In order for users to get a more correct mental model of security they need to learn what risk their data is exposed to. The biggest problem today is that the users do not see the need for security. One approach would be to focus more on the threats and dangers touch phone users are facing and what precautions the user should take to avoid them. The students mentioned that they are influenced by friends and media, and have more trust in service used by the masses. People needs to be informed about the level of risk, but in order for them to really take on that information it needs to come from sources that the users listen to and respect. Which could be the authorities or companies with good reputation. What to inform the users about could for instance be how the context can affect their privacy and which dangers connecting to unprotected wireless networks could offer. In addition which precautions to take to lower the risk.

It can be difficult for the users of an authentication mechanism to understand exactly how it works, and how secure it is. The students feel safer with the screen lock activated, but do not rely entirely on it or feel completely protected. A common belief among the students were that if unauthorized people really want to access their phone, they'll manage with or without a screen lock. A prerequisite for the authentication mechanism to be used is that the users trust it. The students states that they understand that the need for security has increased since the feature phone, but according to their answers it is reason to believe that about half of them do not find the effort of using a screen lock reasonable in relation to what they get back in protection. In stead they trust their own ability to look after their device, and experience the screen lock as unnecessary.

From the interviews and probes I learned that these students do not emphasize security as very important. The reason can be that the mental model has not been able to keep up with the development of the mobile technology. In other words the transfer of knowledge from a mental model for one task to another (20) has not evolved in the same pace. Authentication on touch phones is relatively new compared to authentication on PCs, which is why we probably are not aware of the new threats use of internet in public entails. Using feature phones there were no need to relate to any other form of security then the pin code that were used when the phone was turned on. This in addition to a simple screen lock, which often was described on the display, “press OK and then * to unlock”. The purpose of the screen lock was then mostly to avoid calling or texting anyone by accident when keeping the phone in a pocket or a purse, and can be compared to the sliders that exists on touch phones.

If we use the door as a metaphor everyone understands the need for locking a door, and no one questions this. It is a habit and we do it without thinking. In order for people to activate and use screen locks on touch phones they have to be designed in a way that people don't have to think when unlocking the phone. Questions that can be asked are; does the users need to adapt to the system, or the system be adapted to the user? And can appropriate models be elicited from what users already know, or is it necessary to invent and promote new models?

One attempt used to create an understanding of secure passwords have been to use a password security meter, which gives you an indication of how secure your password is. Security advisor in Evry Consulting, Per Thorsheim (69) states that some security measures provide a false sense of security. During the interviews I experienced that people had more trust in their own ability to create secure passwords and don't really trust password meters. It is no current common standard of how to measure the security of a password. It has therefore emerged many different ways to perform this measurement, and the result will vary based on what password meter that are selected. The interviews showed that people are not completely ignorant to them, but the password security meters are not very essential for which password the users chooses. To check if there were any reason for the students uncertainty regarding password meters, eight different security meters were tested (Appendix 3) with the same password; password@?:-). Not unexpectedly the results varied a lot and generated results all the way from very weak to very strong based on this it understandable that people have trouble relying on them. This is one of the reasons that it is hard for people to get the correct mental model.

When designing for people whether it is on a screen or physical objects it is important to ask; what are the users doing and why are they doing it. When logging in the user are going through an identification and authentication process, but why? There is only one simple answer, to get access to what's inside of the security wall. The authentication in it self is a necessary step to reach a protected goal which can be an application, a web service e.g. This can be compared to the purpose of a travel company. They don't sell people tickets; they get people where they want to be. Exactly like Feide, they don't offer the user a login service; they get people to the educational services that they want to visit. Status today seems to be that people think typing a password or unlocking the screen is stress, takes to much time and that the screen lock

interferes with the task the users wants to perform. As Thorsheim (69) explain that this is because it don't seems necessary and the effort it requires to unlock the service does not seems reasonable.

The users need guidance in order to change their habits, and to get the right mental model the users need help from developers and designer. Standards for for instance security meters should be developed and the technology industry should cooperate and be more coordinated. If the users can recognize a specific authentication mechanism that they are familiar with, on several well recommended services it is more likely that they will trust both the service and the mechanism.

If new mechanisms are introduced the users mental model can be challenged, if it is very different from what the user know and have experienced before. It can take some time for the people to get used to new mechanisms. Using components that people are familiar with from other services can make it easier for them to learn to interact with the mechanism, like text fields or buttons. Focusing on affordance and being consistent will make the interface more intuitive and the users mental model can be easier transferred(22).

6.2.3 Conceptual model

A term closely related to the mental model is the conceptual model. Susan Weinschenk (71) defines it as:

“..the actual model that is given to the user through the interface of the product. The actual interface is representing the conceptual model. Someone designed a user interface and that interface is communicating to you the conceptual model of the product.”

When introducing new types of authentication mechanisms the conceptual model should be preserved in order to make it easier for the users. The goal should be to create a product that do not require instructions, but that the user can learn through interaction. If the conceptual model of the product matches the users mental model the user will experience the design as intuitive and useful and get an overall positive experience (71). A mental model diagram could be a good tool use to when trying to transform the users mental model into a conceptual model.

6.2.4 Mental model diagram

A starting point when creating a good user experience it is to get to know the users motivation for what he is trying to accomplish and what drives the user in general. A mental model diagram is a visual description that will give a detailed view of how certain user groups think and feel and help the designer to create product features that match their mental model (72). The diagram can be structured like towers in a skyline, where the users thoughts, behavior and feelings are represented on the top where each tower represents a cognitive space. Underneath the skyline the product features that try to improve or support the users behavior is placed.

Mental model diagrams can be useful when creating a web site or an application. In figure 6.6 it's made an attempt to create a mental model diagram based on the outcome from the mechanisms, to see how the authentication process can be improved and support the users behavior. The users thoughts and behavior are divided into three towers. Users want instant access to the phones features and apps, and think authentication is stress and that it steals from their valuable time. The first tower displays what the users do to avoid stress and save time. Even if students say they are not too concerned about security the interviews have revealed that they do take some unconscious precautions to secure the content on their touch phone, this is presented in the tower in the middle. The third tower presents how the users behave to stay connected and be available at all times.

Underneath the horizontal line I have tried to come up with some features that would make it possible for the users to go through the authentication process fast and easy without taking shortcuts that affect the security. It is common among students to use the same password on multiple services. One of the reasons for this is that they are afraid of forgetting their passwords if they have too many. Adding a hint will make it easier to remember also more complicated authentication IDs and the user don't have to think that much. Because of small keys typing on a touch phone can be cumbersome and take time, by offering alternative methods that does not requires typing the authentication process can be speeded up. When signing in with Feide, the users are presented with the information about them that will be shared with the service. This have to be approved in order for the user to continue. Assuming this information is important and cannot be removed, it should be shortened and made easier to get the users to read it as they are not interested in spending time reading long user agreements. Short-cuts are already a feature in iPhone, and have the purpose of making it faster for the users to fill in forms, by creating personal short-cuts. In stead of making the user sign in to all types of different web services and applications single-sign on would make it possible for them to save time by only signing in once. Another option is to do like Apple on iOS 5.1 (73) where they have added a short cut to the camera application that enables the user to take without unlocking the phone.

There are several ways one can support and improve the security of the phone. Some content on a touch phone are more sensitive than other. One informant, without a screen lock, mentioned for instance that the person would have liked to have a lock only on her images. Such a feature would have enabled her instant access to low risk content like games or news applications, while more sensitive and high risk content could have had a higher security level. If the phone were able to recommend security levels based on the content it would have been much easier for the user to adjust the security settings. Similar recommendations could also be offered for different contexts that may pose varying risks.

Today it takes an effort from the users to activate the screen lock, there are reason to believe that more people would have had a screen lock if it was activated by default. Users have a good reason to not trust password security meters. When the users don't trust they will not have the intended effect which is to help the users create more secure passwords. In order for

people to trust them there should be made standards that are widespread among known services and they should be marked for users to easy recognize them.

We are online all the time and are eager to check the phone to see if there are any updates or exiting news. One of the informants commented during an interview that the touch phone had made the person addicted to the e-mail, and that she checks it all the time. By activating haptic or sound notifications the users does not have to check their phone all the time, because they will get feedback when something happens.

Mental Model Diagram

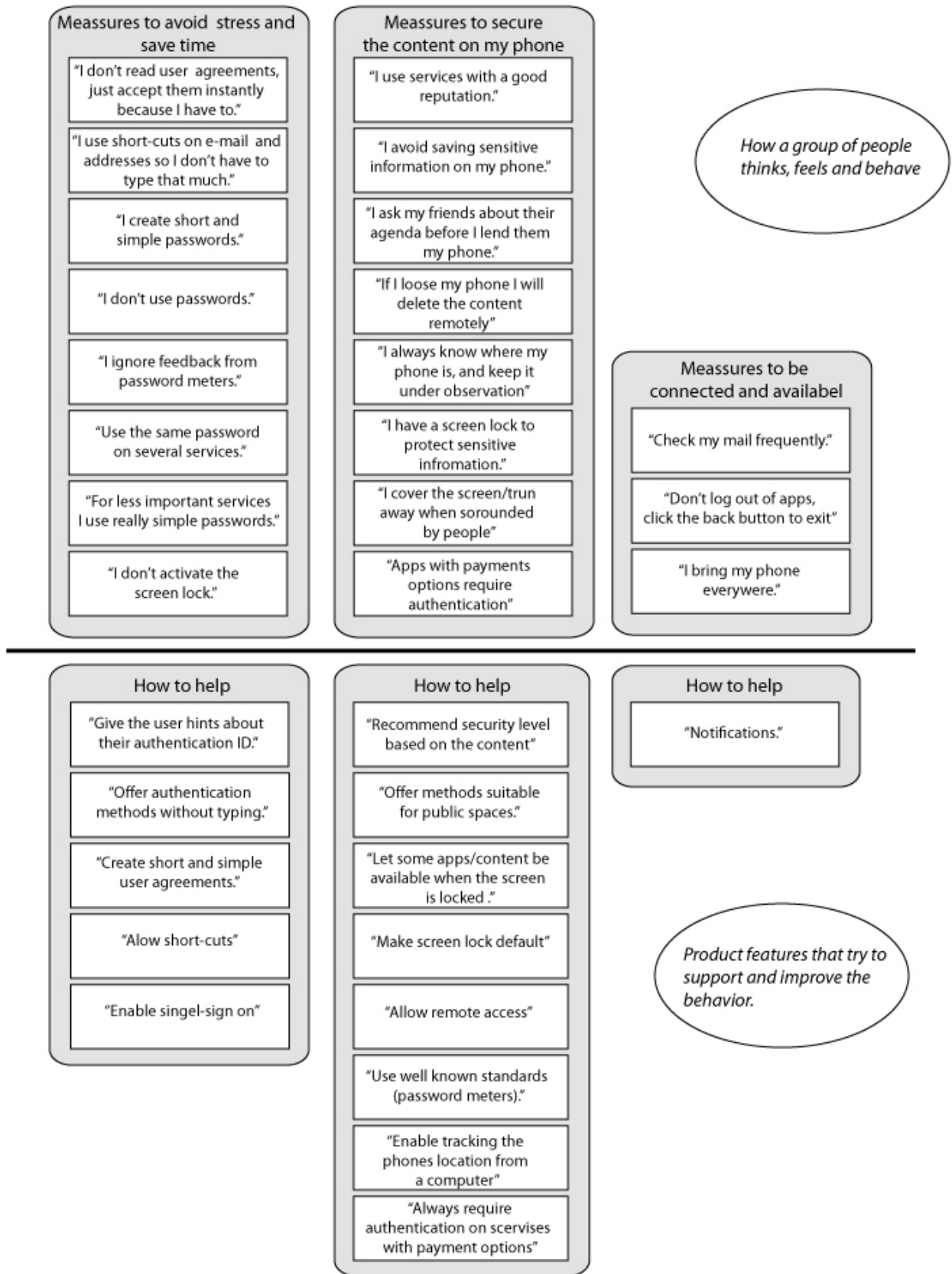


Figure 6.6 Mental Model Diagram (72)

The top of the diagram gives an impression of the users mental model. Based on that knowledge the mental model diagram can support the development of intuitive and user-friendly product, by ensuring that the user always is in focus. With this model we have been able to induce specific requirements that can improve the user experience.

6.3 Eye tracking on touch phones and of authentication mechanisms



How can eye tracking and eye tracking software be used as a tool to investigate authentication mechanisms on touch phones?

Eye tracking are being used for several purposes, both as assistive technology and as a testing tool. It's the latter that have been the focus in this project. The Norwegian Computing Center⁶ are doing a lot of research within the areas of information and communication technology and recently used funds on equipment that facilitates eye tracking on mobile devices. As I am relatively new to eye tracking I will look at this method from a beginner's perspective. I will discuss the problems and challenges emerging from the method and which interesting findings that could be extracted from it. At the end I will discuss how eye tracking will works as a tool for investigating authentication mechanisms.

6.3.1 Challenges and problems

There are many factors that come into play for eye tracking to be successful and accurate. Eye tracking on mobile phones can in many ways be more challenging then eye tracking on a stationary computer. Some of the challenges were known and predicted in front, while others were revealed during the testing. In order to track the eye movement the phone must be mounted on a tripod and the cameras need to be calibrated to the screen and the users' eyes. Even though the flexibility for the equipment and tripod have been improved it will still not give the user the same experience as if the phone was lose and they could hold it in their hands.

To see the screen on the recording it is important to make sure that it is not too light or dark. This can be fixed by adjusting the light in the room or the display backlight. It is also important to make sure the screen is in focus to get the most out of the eye tracking data. A known issue is that due to reflection in the glass, people with eyeglasses can be difficult to track, and also people with an Asian background can be difficult to get a track record with high quality because of the

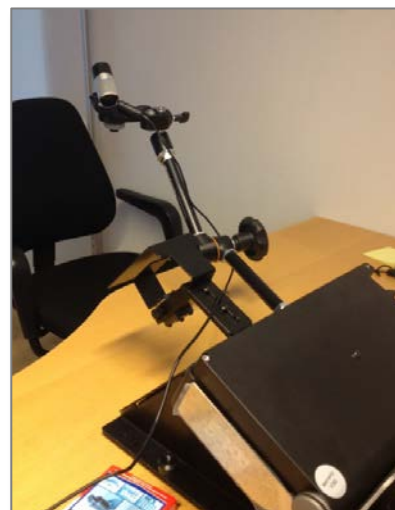


Figure 6.7 Eye Tracking

6

www.nr.no

characteristics of their eyes. In this project none of the students wore glasses and I did not experience any issues when tracking people with Asian background.

When doing eye tracking it is interesting to compare the result of different users and look for patterns and create heat maps to discover trends among the users. However, a prerequisite for being able to do this probably turned out to be that all of the users had the same starting point. It would therefore have been an advantage if the same phone was used throughout all of the tests, and that the tests were conducted either only with a horizontal or a vertical screen as the content is presented differently depending on the rotation.

Because the prototype and Feide login was not adapted to the size of a mobile screen the users several times needed to use their fingers to zoom in on the screen. This action made it more difficult to compare the eye movement as the content on the screen also appears differently according to the level of zoom. Pop-ups like keyboard and lists are different based on the operative system on the phone, and a comparison may lead to an incorrect image of the reality.

On touch phones the interaction is depending on the user to place its finger on the screen. As the finger will cover parts of the screen it can be seen as a disturbing element during the eye tracking.

The distance between the eyes and the phone is also important in order to track the informants' eyes correctly. An issue that arose was that the participants were used to hold their phone closer than the equipment allowed, they kept leaning forward to look at the screen, and had to be asked to lean back. To get the best tracking result Tobii recommends a distance of approximately 60 cm from the informants' eyes to the test object (74). Especially when the users were typing or reading a longer text this distance was experienced as too long for the users. Because they leaned forward instead of zooming this affected the quality of the eye tracking.

To sum up there are several issues that one has to be aware of when performing eye tracking on touch phones:

- Make sure the screen is in focus before the testing starts.
- Avoid using informants with glasses and be careful with people with narrow dark eyes.
- If creating a heat map, use the same device on all participants and avoid moving the device and camera between the sessions.
- Decide in front of the session if the screen should have a horizontal or vertical view.
- Avoid pages that demand a lot of text input as the typing will take time and the screen is covered by the on-screen keyboard.
- Make sure the informant is sitting in a comfortable chair, and pay attention to their

distance to the screen which should be approximately 60-65 cm.

These are all factors that can affect the result, and when analyzing the eye tracking data all these issues have to be taken into account.

6.3.2 Interesting findings

In addition to the challenges that emerged from the method there are also possible to get interesting findings from eye tracking on touch phones.

Through interviews and talk-aloud walk troughs one can get to know a lot about how the user think, observation alone is also an efficient way to learn how users interact with an interface. Through a normal observation it is hard to tell if the users attention is drawn to certain design elements if he is not clicking on them. With eye tracking one are able to both observe the user and also see what's happening in-between the interaction. This knowledge can help the designer to uncover usability issues and thus create a better flow (7).

Eye tracking data does only trace what the users are looking at, not why they are looking at certain elements. Because of this limitations the method should preferably, as all methods, be used in combinations with other methods. In this project the eye tracking were combined with short interviews after each session, which generated some interesting findings.

It was revealed early into the project that time and efficiency are critical for the users in an login process. We already know that writing on touch devices can be cumbersome, and also got this confirmed in several interviews. As opposite to older phones or a computer, where you type with physical buttons, you cannot feel the buttons on a touch screen. This makes it almost impossible to write without looking at the keyboard. The focus must therefor constantly switch between the keyboard and the text field. Because of the short distance between them this is not an immediate disadvantage. A couple of informant did have to try more then once before they complete Feide login, even if this was a username and password combination they where familiar with. This proves that the on-screen keyboard can create difficulties even for experienced users.

If we measure efficiency in number of fixations on the screen before an action is complete, one could say that the pattern authentication with direct manipulation were more efficient. In spite of this the users still rated the password authentication highest. The pattern was also rated high, but the users did still preferred the password. This brings us back to Krug's definition of usability and his second law where he states that "it doesn't matter how many times I have to click, as long as each click is a mindless, unambiguous choice (15)". It is easy to draw parallels from the physical interaction with a site, like clicking, to how the eye interact with a site. The user testing together with the interview confirms that it doesn't matter how much the gaze needs to wander over the screen as long as the user don't need to think and can perform its tasks mindlessly and unambiguously.

Today usernames and passwords are typed in everywhere, and often also the same combination on several services. The users are familiar with the keyboard, and know exactly

where to find the different letters, which means that even if the gaze are moving a lot, it does not necessarily indicate that the user is confused. It can for instance indicate that the password contains a lot of letters. Looking at the time it takes for the user to authenticate himself can be just as valuable as looking at the gaze plot when looking for the ideal method. Especially in this case were the students valued fast and easy access as important.

The image and sound authentication were performed the exact same way because the sound did not work in the mobile browsers, but there were some differences in the design. The findings revealed that the students gaze wandered more when the user performed the sound authentication. This difference made it interesting to take a look at the interface to see if there were visible differences that could affect be the reason for this.

Comparing the two methods we can see that the main difference is that the pictures on image authentication is displayed with a white background without a label, while the pictures on sound authentication have grey background and labels. The images is also larger and are separated with a wider padding. The differences in the gaze plots gives hint that using a white background can make it easier for the users to separate images, and that removing the label under the images could have been an effective measure in order to improve the user experience. Another solution could be to increase the size of the labels and images could also be a possible solution.

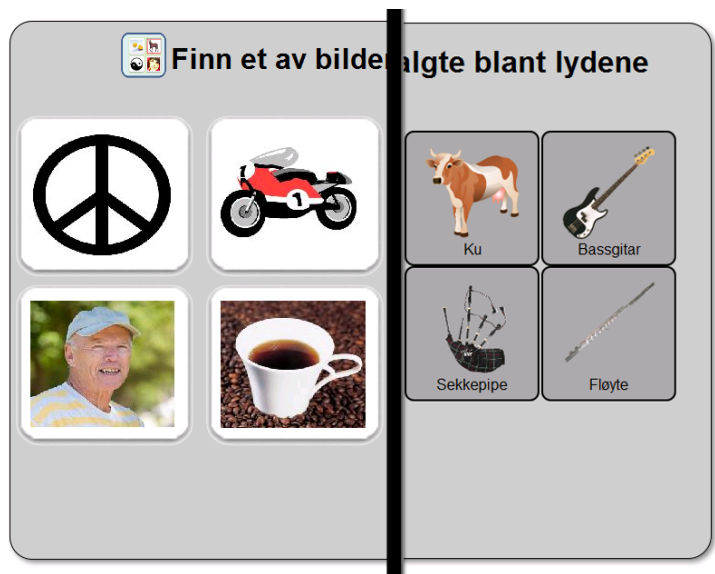


Figure 6.8 Image vs. Sound authentication

Krug's third law tells the designer to get rid of half the words on each page, and then get rid of half of what's left (15). The advantage of mobile adapted websites and applications is that designers seems to have realized that they need to think differently when designing for the mobile screen. The size of the screen have for instance forced them to be more focused, get rid of obsolete information and concentrate on the main functionalities (75).

In the prototype each method were introduced with a short description. The eye tracking data visualized that the informants were all reading the first descriptions carefully, but the further into the session they got the less careful. Users don't want to waste time on things they think they don't need(7), which is probably why they did not read the complete description of the password and question authentication. The user are familiar with password authentication, and have clear a clear view on what to expect from this mechanism, questions are also common to use as a security in case the password is forgotten. The users were at the end of the test asked if they got enough information to complete the test, where they all agreed. As for all user testing the context needs to be considered when looking at the result. The informants often

feel that they are being tested and not the product, this can have led them to read the descriptions more careful then they would have in another setting.

In the testing of Feide login the informants used did not have to come up with a new password, but used their regular combination when accessing services provided by the University. Most of the users had previous experience in using Feide and was therefor probably more relaxed which was why they did not read the agreement before they confirmed it.

The questions took longer to set up then the other methods, and the users needed additional explanation when setting it up. One reason for this can be that the informants did not read the description thoroughly enough because they assumed they knew what to do. Even if the header said that they were suppose to create three questions, none of the informants had seen this. From the eye tracking data we could see that the informants were not fixating much on the header before their gaze went straight to the input field, open fields like this is what Nielsen and Pernice calls magnetic UI elements (7). Even if it was written in large letters it did not manage to take the attention from the input field, that information could have been even more highlighted. The actual implementation of the method did in spite of this not take noticeably longer time, but the users still rated it low on the evaluation at the end. The interview confirmed that the reason was that they did not trust the method to be very safe.

Knowing that movement attracts attention it was not unexpected that users paid attention to the progress bar in the address field of the browser. What the eye tracking data also showed was that they immediately after finishing a task moved their gaze to the top of the screen. This even before the progress indicator were visible. The reason for this is that the informants had learned through previous use how the progress indicator behaved and expected this action. If there were any important information the users needed to be informed of while waiting for authorization this could be a place to put it.

During the interviews the informants commented that they did not see any large difference between the password and image authentication; “it’s the same principle, four numbers, four images, it’s exactly the same”. After the users had tested and rated both mechanisms, the impression had changed and the password authentication came out as a clear winner. It took the informants longer to authenticate with images, and most of them were a bit skeptical about this mechanism. These findings points out what mentioned earlier that the best results comes from combining several methods, and that user testing is essential.

To sum here is an overview over some of the interesting findings that were generated from eye tracking on touch phones.

- Eye tracking can help to uncover general usability issues and thus create a better flow.
- The eye is attracted to movement
 - The students followed the loading bar at the top of the screen.
- According to the mind-eye hypothesis people are usually thinking about what they are looking at.

- The data must however be analyzed as it does not say anything about why the user is doing what it does.
- A lot of fixations on elements of direct manipulation can indicate confusion.
- When typing it is normal with a lot of fixations.
- Many options generates more fixations on the screen before the user find and select an options.
- Efficiency should not only be measured in number of fixations, the time it takes to perform an action can be just as informative.
- People ignore things they think they know and don't need in order to perform their tasks.
- The user does not always do what he says he does – use multiple methods to get the total picture of the users behavior.
- The users experience will affect how well an action is performed and enable the user to more easily be able to predict the next event.

These are all generated from the eye tracking on touch phones. Findings concerning general usability did confirm that what Nielsen and Pernice had written about eye tracking on terminals like stationary computers and laptops in many cases also apply to touch phones. When doing eye tracking on authentication mechanisms there are additional considerations one need to have in mind.

6.3.3 Eye tracking of authentication mechanisms

In addition to the physical considerations there are ethical issues related to eye tracking of an authentication process. The information that the user are typing in is person sensitive and eye tracking will capture this information on video, which can make it possible for unauthorized users to abuse if they get hold of it. The informants were informed that the eye tracking data would not be forwarded to any third parts and signed a consent before the testing started. After the test was conducted the informants were asked if they were affected by their actions being captured on video, but all commented that it did not influence them any further. That all the students knew me did probably have an impact on their experience of safety. The e-Me prototype was new to all of the users, and everyone created new “test-passwords” as their normal passwords did not necessarily fit the conditions for the prototype.

The authentication mechanisms that were tested within this study were run on two different websites. Input fields on a phone needs to be of a certain size for the users to see what they type, and the on-screen keyboard occupy the rest of the screen. There are rarely room for any other distracting elements like ads. The user interface on the prototype and Feide login were fairly simple and did not contain any ads or other elements that were not relevant to the user. This made it easier for the informants to add input without being distracted. Even if the interface initially contains no distractions, pop-up notifications and phone calls will appear unannounced, and can come at an inconvenient time. The eye tracking were done inside in a quiet environment, in a normal use situation the user could also be distracted by the surroundings.

A challenge when doing eye tracking of authentication mechanisms is that each users will have their own personal password, pattern or image combination. Even if they were using the same phone, with the same rotation e.g. they would not be entering the same input. Therefore it can be hard to compare authentication mechanisms. In the e-Me prototype it was predetermined that the password should contain six characters, and both numbers and letters, the pattern should only contain six points, and there should only be four images and sounds. With similar conditions for all the users it will become a more appropriate comparison.

6.4 How to create accessible authentication mechanisms?



In what way can we create accessible authentication mechanisms on touch phones?

The forth part of this assignment is focusing specially on accessible design on mobile phones. I will look at the concepts of universal design and adaptive information systems and how these can be applied to the process of authentication on a mobile touch interface.

6.4.1 Universal Design and Adaptive Information Systems

There are several ways of making sure that people with disabilities are included and can use a product. In this section I will look at two design terms, universal design and adaptive information systems that have been described in the theory chapter.

It is argued that there is no currently such thing as a universal designed authentication mechanism (39). As mentioned earlier designing for everyone is a challenge, an approach have been to make decisions based on what are suitable for the general population, in order to reach out to as many as possible. Looking into blind and visually impaired as a user group, I have found that it is very hard to define their needs. This is a very heterogeneous group of people; as there are numerous degrees of visually impairments. It is also common to have a combination of several disabilities. In theory, if one should offer alternatives to all the different disabilities and combinations of them, it had to be created an infinite number of solutions.

When designing for people with disabilities, personas is a common approach in addition to following the web standards and use online testing tools. Personas represent the target group for the service and are not real users but fictional portraits of users that presents what we know about real users. Personas can help making decisions about the services goal, content, functionality, form and accessibility to a certain extent, but will never be able to replace real users (76). People are complex and there will always be someone that does not fit the profile of the personas, especially when targeting people with disabilities. There are taken steps to improve the user experience for all users, including disabled. Universal design is one of these approaches.

According to the Center for Universal Design at North Carolina State University (77), universal design (UD) aims to create products and environments that are usable “by all people, to the greatest extent possible, without the need for adoption or specialized design”. Normally users are only offered to login with one single authentication mechanism and no optional alternatives. This one option should ideally follow web standards and accessibility guidelines; to make it easier for users that are depending on assistive technology. It is important to note that universal design does not eliminate the need for assistive technology, but should reduce the need for it and its total costs.

Even if the goal with universal design is trying to include everyone; ironically enough can this lead to exclusion of some individuals. The Disability Rights Commission found that only 45% of the problems connected encountered by disabled users were not violations of the guidelines in WCAG 1.0 (78). This proves that it is not enough to stick to the recommended standards, as a lot of the usability issues will not be discovered unless the product is tested on real users, and preferably a heterogenic group of users. There are probably as many varieties of disabilities as there are individuals with disabilities. In addition there are also large varieties of assistive technology that it can be difficult to adapt to. This is why the best way to meet most users and their needs could be to focus on designing authentication mechanisms that contains several channels, modalities and adaption options for various user needs (39).

Principle number two about universal design (77) points out that the design should be flexible in use, and accommodate a wide range of individual preferences and abilities. In other words the design should be adaptable to different needs. Three different approaches to adaptive information systems were presented in the theory chapter; multimodal interface, user-controlled identity management systems and profiling.

User-controlled identity management systems focuses on users ability to edit their account and decide what personal attributes that should or should not be revealed. This requires that the system knows who the user is, thus the user needs to identify it self through a logging process.

Profiling can as mentioned be divided into group profiling and personalized profiling. Personalized profiling is a profile connected to one specific person and his or her needs. It can for instance contain personal details about medical health and disabilities. This type of personal content needs to be protected and will require the user to be authorized to enter or edit information.



Figure 6.9 TV2 Skole – Sign Language

The pilot project Tabia is an example where personalized profiling is used. Tabia made it possible for students with visual impairments, hearing disabilities and others to adapt media

content at TV 2 Skole to their personal needs. In order for hearing-impaired persons to benefit from the video in the same degree as hearing people would, the speech can be interpreted into sign language or subtitles must be added. The project let the students define their preferences in a centralized preference module, and the services automatically retrieved the correct settings after logging in.

To use personalized profiling in an authentication situation would be inappropriate as the user then most likely would have to specify a lot of personal details before an suitable authentication mechanism would appear. This would make the process of logging in unnecessary time consuming and cumbersome, and the user would probably also have to ask for help to complete it. These two types of adaptive information systems requires the user to be logged in and do not include the authentication process itself. These concepts would therefore not solve the problem with inaccessible authentication mechanisms.

Group profiling on the other hand are more general and aims to support specific groups of users, like blind or cognitively disabled. Group profiling can be very valuable for people with disabilities, but because profiles like this are very general there will always be someone's needs that are not covered. Group profiling used in an authentication setting could have been carried out by the user specifying what group he belonged to before he was directed to an authentication mechanism intended for that specific group. From previous research it has been clear that people does not want to be stigmatized based on their disabilities which would be a problem in such a setting (41). Another issue would be that because of the large variety within each user group it is still unlikely that one type authentication mechanism would be suitable for everyone.

Multimodal user interface is the last approach that were talked about within the field of adaptive information systems. A flexible multimodal user interface can meet different user's needs, abilities, situations, preferences and devices by making it possible for users to adjust the product settings based on their needs, and choosing between multiple ways of control and experience the content (41). On a MediaLTs seminar about accessibility and user testing it was stated that in order to treat everyone equally one needs to treat everyone different, because people are different (79)! Based on this statement a flexible multimodal user interface would seem like a reasonable solution.

Transferring the practice from Tabia to an authentication situation would be challenging. At TV2 Skole you sign in and because the service already knows who you are, it can easily go and get the specified preferences, but before the user has been authenticated this information is not available. Users are generally skeptical about informing the system about their disability even

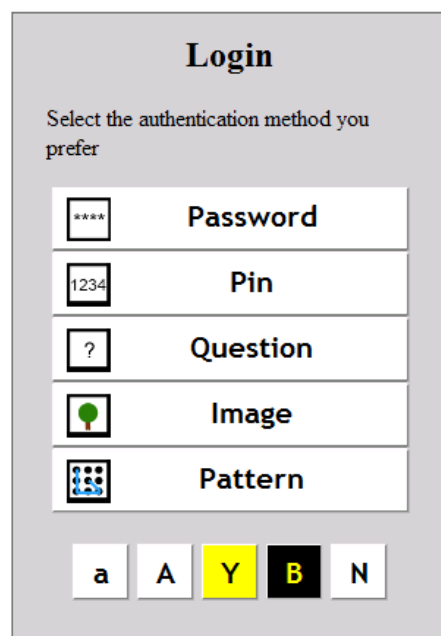


Figure 6.10 Multimodal authentication

if they do not normally hide it (41). Instead of asking the users to reveal their disability it is more appropriate to allowing them to choose between different presentations of the content. The alternative could therefor be that the user select preferred authentication mechanism on every login. It could look something like Figure 6.10. Using cookies, the mobile browser can remember your choice without storing any other personal information, and are not actually connected to the user, only to the phone.

6.4.2 Multimodal authentication on touch phones

Most articles about this are only looking at the use of computers. When focusing on mobile phones it may be relevant to look at how user needs change based on the various use of the devise, and not only user needs in general.

According to W3C Multimodal Interaction working group all users benefit from being able to choose which modalities they find convenient in any situation (80). Multimodality has the potential of being beneficial for both disabled and non-disabled people. As an example do people appreciate subtitles of films if they do not understand the language, but also those familiar with the language enjoy films with subtitles in the original language. Another example is that voice output and text information benefits seeing people in situations in which the visual channel is not available for reading, such as when driving a car.

Mobile phones are used in a number of different situations and locations. Giving people an opportunity to choose between different authentication mechanisms will give them the opportunity to adopt the method to the context they are in. All people will at some point in life, of various reasons and also experience some form of disabilities. Several modalities will in addition enable the user to adapt the method to their current physical context.

7 Conclusion

The main objectives in this thesis have been to provide new knowledge about authentication mechanisms on touch phones. This has been done by reviewing existing mechanisms and exploring people's mental model of security through interviews and user testing. In addition to this I examined how one could approach authentication mechanisms in order to make the login process accessible. Ultimately I should have a good basis to answer the research questions, starting with research question 1 where I did a review of a selection of authentication mechanisms.

7.1 Review of authentication mechanisms on touch phones

This has had a theoretical focus as well as empirical studies. To get an overview of what authentication mechanisms that were used on touch phones today I did a review of eight authentication mechanisms and screen locks. The different authentication mechanisms used in this thesis were found through online research in articles and by exploring different operating systems on touch phones. From the probes and interviews it became clear that most people don't turn off their phones, or log out of applications. Because of this it was relevant to review screen locks in addition to regular authentication mechanisms as this often are the only mechanism protecting the phone. The mechanisms were reviewed based on W3C recommendations for user input in Mobile Best Practices 1.0 (27), and the concepts of direct manipulation and context as these are what separates authentication on touch phones from stationary terminals with GIMP interface. Some of the features that the informants meant was important for authentication mechanisms were efficiency and if they are easy to remember, these qualities were also included in the review.

All mechanisms have their drawbacks, and security is often implemented on the expense of the usability of the system. Mechanisms that rely on direct manipulations and natural gestures, like pattern, image gestures and the piano, will probably be easy to learn and efficient to use, but this sort of interaction is often visible by others and can therefore be insecure in some contexts, as they could be easy to copy. Typing on a touch screen can be cumbersome, and inefficient, but the users trust this method and it is also less visible to others as the characters are hidden. Biometrics that are relying on something the user has could be secure, as the user might not have to remember anything particular, but the technology is still inaccurate which makes it insecure if the mechanisms are not combined with other types of authentication. The proximity-based and NFC mechanisms would be easy to use, and efficient as the phone is unlocked without direct input from the user, but the disadvantage is that the tokens can be stolen or lost.

It is hard to define the risk level of a mobile phone as it depends both of the content and the context of use, but most of the mechanisms that were reviewed could only be qualified as security level 1. The slider and circle mechanisms are easy to use, but not secure if they are not combined with other mechanisms. Don Norman states that more security not necessary need

to make things more complex or less attractive to use. One of the issues with authentication mechanisms that have a high level of security is that the users in many cases need to remember and type in a lot of information. An approach to reduce the number of keystrokes could be to explore other types of input than text input that rely on recognition rather than recall, where it probably is a lot of undiscovered possibilities.

7.2 Mental model of security

The second part of this thesis was to examine the term mental model of security and discuss how we could utilize the concept of mental models in design of authentication mechanisms for touch phones. In order to answer this research question it was essential to get to know the target group, which in this case were students. This was done through probes, interviews and user testing. Instead of evaluating a specific product I took a step back and focused on the users behavior and why they behaved in certain ways. In total 11 informants were included in the study and this made it possible to see trends among them regarding their mental model of security. A mental model is based on the users knowledge and experience and the mental model that the students had of a touch phone were colored by their experience from feature phones and PCs. The users do not trust the screen locks entirely and many students chose not to activate it to avoid stress. Most of the students states that they are not too concerned about the security and that they are able to keep the phone safe without any locks. As the content on a touch phone increases the need for security measures also increase, but the users mental model does not seem to evolve according to these changes, which can result in a lower level of security than what should be required.

Users need help from developers and designers to get the right mental model. As a step towards a conceptual model that matches the users mental model, I created a mental model diagram based on the knowledge of the users and their behavior and thoughts. It proposes among other things to offer authentication mechanisms without typing, to make sure the process will be easy and efficient. In addition to keeping the user updated on the what security level should be used, according to the content.

7.3 Eye tracking on touch phones and of authentication mechanisms

As a part of this thesis there were conducted eye tracking with five informants testing different authentication mechanisms on their touch phones. This testing was conducted to see how eye tracking and eye tracking software be used as a tool to investigate authentication mechanisms on touch phones. The informants tested both the prototype from the e-Me project and Feide login where they accessed the University service Vortex. The user testing revealed that many factors need to be considered in order to conduct a successful eye tracking, especially regarding the technical implementation. As observation with eye tracking only are able to communicate what the user look at and how the person is interacting with the screen it is necessary to combine this method. Or else it would for instance be difficult to figure out

whether the user is confused, or just looking at an element because the person is interested or finds it relevant, one also need to talk to the users.

From the testing I learned that in order to create heat maps and compare data from different tests the setup should be similar in all the tests, and the user should avoid having to zoom in order to get the most accurate result. Eye tracking is a good tool to uncover usability issues. There were differences in the gaze plots from the image and sound authentication. By taking a closer look at the interface I managed to find things that could be improved in the design, which might also improve the user experience. It could be easy to draw a conclusion that a lot of fixations indicated that the task were not performed efficiently, and that the user would not be satisfied. In some cases could this be a correct assumption, but during typing one probably have to expect a lot of fixations because the gaze are moving between the keyboard and the input field. Inspired by Krug's second law (15) I would dare to state that it doesn't matter how much the gaze needs to wander over the screen as long as the user don't need to think and can perform its task mindlessly and unambiguously.

Opposite from websites, mobile apps or sites are often simpler and don't contain a lot of distracting elements. This was also the case when the authentication mechanisms where tested. Users are attracted to input fields, which can take the attention from other text, and result in los of important information. When doing eye tracking of authentication mechanisms a challenge is that users can have passwords of different length and content, which can make it irrelevant to do a comparison. Whenever conducting user tests with eye tracking it is important to inform the participants of the purpose of the study. Especially when the the study rely on sensitive data, the participants needs verification that the data will be treated confidentially. One reason is to make them relax and get the most naturalistic data as possible.

7.4 How to create accessible authentication mechanisms?

The last part of the thesis investigated the concepts of universal design and adaptive information systems, in order to discuss how we can create accessible authentication mechanisms on touch phones. Universal design aims to create products and environments that are usable by all. Blind and visually impaired are a heterogeneous group of people. Using personas, web standards and online testing tools will uncover a lot of accessibility issues, but there will always be someone that does not fit the profile and are excluded. It's been argued that it does not exists a universal designed authentication mechanism, because of the large diversity of users. Looking into adaptive information systems like user-centered identity management systems, profiling and multimodal user interface it has been clear that only the last one would work in the users first meeting with a system. Because user-centered identity management and profiling are depending on knowing the users identity in order to adapt, a multimodal user interface would be more appropriate to use in an authentication setting. This could enable the user to chose between different authentication mechanisms, this would not only be convenient for users with disabilities, but would also enable the user to adapt the method to their current context.

7.5 Further work

A lot of concepts have been covered in this thesis, but there are still areas that would be relevant to look further into and include in a more extensive study of this field.

The review were made on a selection of screen locks, and were based on theoretical concepts and user interview. User testing of these mechanisms, maybe in different contexts could have given a more complete picture of them, and made it possible to reveal more problem areas. In order to work towards attractive authentication mechanisms that also are secure it would be relevant to do closer research on mechanisms that not are based on text input, and rely on recognition rather than recall, like e-Me's image authentication.

Valuable insight about students mental model of security were provided through this study, and organized into a mental model diagram. This could be a good starting point for conceptualizing new ideas for authentication mechanisms. Create a prototype that could be tested on students, where some of the suggested features were implemented would be essential in order to see how design based on user's mental model works in practice.

One of the product features were generated in the mental model diagram was; recommend security level based on the content. It have been discussed that the need for security increases in parallel with number of applications and services one can acces on the phone. One way to get people to activate a screen lock could be to come with recommendations based on number and type of applications, or the context of use. Recommendations could be communicated as notifications like this:

- “You have over 30 apps and should consider to activate your screen lock. Go to settings to activate it.”
- “You have over 100 apps and should consider changing your screen lock from pin to a pattern with more then 6 points. Go to settings to change screen lock.”
- “You are using several apps that can contain personal information of you. You should activate your screen lock. Go to settings to activate it.”

The motivation for the users to activate the a screen lock would be the increased amount of personal content on their phone. These notifications from the manufacturer will come from a source that it is more likely that the user rely on, and may therefore increase the chances that they will follow the proposed recommendations. Notification could also work as a tool for learning, and improve their understanding of the need for authentication and security. As for further work it would be interesting to do some user testing to see if this claim is correct. I have been doing some briefly research for similar solutions but have not discovered anything per date.

There are a lot of interesting information about people with various disabilities in general, but not about how they relate to touch interface and particularly authentication mechanisms on touch interfaces. This is something it would have been interesting to do more research on. User testing with disabled participants were not prioritized in this thesis, but it would be a

natural next step to implement and test a multimodal user interface for mobile, on both disabled and non-disabled students in order to test the assumptions that were made in relation to research question 4 that multimodal user interfaces would benefit all users.

8 References

1. How the smartphone is killing the PC. the Guardian [Internet]. 2011 Jun 5 [cited 2012 Jan 9]; Available from: <http://www.guardian.co.uk/technology/2011/jun/05/smartphones-killing-pc>
2. Is your business strategy as mobile as your customers? : | : STUDIO NORTH blog [Internet]. [cited 2012 Apr 12]. Available from: <http://blog.studionorth.com/2012/02/09/is-your-business-strategy-as-mobile-as-your-customers/>
3. Phones Generated 10% Of Internet Traffic Last Year [Internet]. [cited 2012 Mar 16]. Available from: <http://www.sitetrail.com/2012/03/08/phones-generated-10-of-internet-traffic-last-year/>
4. Jung H, Stolterman E, Ryan W, Thompson T, Siegel M. Toward a framework for ecologies of artifacts: how are digital artifacts interconnected within a personal life? Proceedings of the 5th Nordic conference on Human-computer interaction: building bridges. 2008. p. 201–10.
5. Design Guidelines on the Security Feedback provided by the “Things” [Internet]. [cited 2012 Jan 9]. Available from: http://www.utrustit.eu/uploads/media/utrustit/uTRUSTit_D2.6_Design_Guidelines_on_the_Security_Feedback_provided_by_the_Things_Final.pdf
6. The Protection of Information in Computer Systems [Internet]. [cited 2012 Jan 10]. Available from: <http://mit.edu/Saltzer/www/publications/protection/index.html>
7. Nielsen J, Pernice K. Eyetracking Web Usability. 1st ed. New Riders Press; 2009.
8. Networked Society “On the Brink” [Internet]. 2011 [cited 2012 Jan 9]. Available from: http://www.youtube.com/watch?v=R7cuatm_bqw&feature=youtube_gdata_player
9. Mobile Website Design [Internet]. Accuracy Solution. [cited 2012 Jan 9]. Available from: <http://www.accuracy.com/Services/Websites/Mobile-Website-Design.aspx>
10. Web Accessibility Initiative (WAI) - home page [Internet]. [cited 2012 Feb 15]. Available from: <http://www.w3.org/WAI/>
11. Web Content Accessibility Guidelines (WCAG) 2.0 [Internet]. [cited 2012 Jan 10]. Available from: <http://www.w3.org/TR/WCAG20/>
12. Fuglerud K, Dale O. Secure and Inclusive Authentication with a Talking Mobile One-Time-Password Client. Security Privacy, IEEE. 2011 Apr;9(2):27–34.
13. Sharp H, Rogers Y, Preece J. Interaction Design: Beyond Human-Computer Interaction. 2nd ed. Wiley; 2007.

14. Yong PL, Saunders RS, Olsen LA, Care I of M (US). R on V& S-DH, (US) NAP. Toward Better Usability, Security, and Privacy of Information Technology: Report of a Workshop. National Academies Press; 2010.
15. Krug S. Don't Make Me Think: A Common Sense Approach to Web Usability, 2nd Edition. 2nd ed. New Riders Press; 2005.
16. Fling B. Mobile Design and Development: Practical concepts and techniques for creating mobile sites and web apps. 1st ed. O'Reilly Media; 2009.
17. Nielsen J. 10 Heuristics for User Interface Design [Internet]. [cited 2012 Jan 18]. Available from: http://www.useit.com/papers/heuristic/heuristic_list.html
18. Saffer D. Designing Gestural Interfaces: Touchscreens and Interactive Devices. 1st ed. O'Reilly Media; 2008.
19. Carey, Susan. Cognitive Science and Science Education. [Internet]. [cited 2012 Apr 5]. Available from:
http://www.eric.ed.gov/ERICWebPortal/search/detailmini.jsp?_nfpb=true&_&ERICExtSearch_SearchValue_0=EJ360280&ERICExtSearch_SearchType_0=no&accno=EJ360280
20. Martin G. Helander, Thomas K. Landauer, Prasad V. Prabhu. Handbook of Human-Computer Interaction [Internet]. second, completely revised ed. The Netherlands: Elsevier Science B.V.; 1997 [cited 2012 Mar 1]. Available from:
http://www.elsevier.com/wps/find/bookdescription.cws_home/524988/description#description
21. Winograd T. Bringing Design to Software. 1st ed. ACM Press; 1996.
22. Mental Models, Metaphor and Design [Internet]. [cited 2012 Apr 26]. Available from: <http://www.syntagm.co.uk/design/articles/mmmad.pdf>
23. Halback, Till, Hellman, Riitta, Rødevand, Gro Marit, Solheim, Ivar. Utformingsveileder for kognitiv tilgjengelighet av elektroniske tjenester og innhold [Internet]. [cited 2012 Mar 9]. Available from: <http://iktforalle.no/veileder-hele.html#standard-elmer>
24. Norman DA. THE WAY I SEE IT When security gets in the way. interactions. 2009;16(6):60–3.
25. About W3C [Internet]. [cited 2012 Jan 10]. Available from: <http://www.w3.org/Consortium/>
26. Mobile Web Best Practices 1.0 [Internet]. [cited 2011 Jun 11]. Available from: <http://www.w3.org/TR/mobile-bp/>
27. W3C. Mobile Web Best Practices 1.0 - Input [Internet]. [cited 2012 Apr 19]. Available from: <http://www.w3.org/TR/mobile-bp/#d0e2028>
28. Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor [Internet]. [cited 2012 Apr 11]. Available from: http://www.regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/eID_rammeverk_trykk.pdf

29. Regjeringen. 4 Sikkerhetsnivåer for autentisering og uavviselighet [Internet]. 2008 [cited 2011 Apr 17]. Available from: <http://www.regjeringen.no/nb/dep/fad/dok/lover-og-regler/retningslinjer/2008/rammeverk-for-autentisering-og-uavviseli/4.html?id=505929>
30. Single Sign-On [Internet]. [cited 2012 Mar 28]. Available from: <http://www.opengroup.org/security/sso/>
31. OpenID - Wikipedia [Internet]. [cited 2011 May 26]. Available from: <http://no.wikipedia.org/wiki/OpenID>
32. What is OpenID? | OpenID [Internet]. [cited 2011 May 26]. Available from: <https://openid.net/get-an-openid/what-is-openid/>
33. Android - Introducing Ice Cream Sandwich [Internet]. [cited 2012 Mar 8]. Available from: <http://www.android.com/about/ice-cream-sandwich/>
34. Mange veier inn - en studie av alternative innloggingsmekanismer [Internet]. [cited 2012 Feb 15]. Available from: http://www.duo.uio.no/publ/informatikk/2011/127955/desserud_master.pdf
35. Bokmålsordboka | Nynorskordboka [Internet]. [cited 2011 Dec 6]. Available from: <http://www.nob-ordbok.uio.no/perl/ordbok.cgi?OPP=autorisere&begge=+&ordbok=begge>
36. What is authentication? [Internet]. [cited 2012 Mar 16]. Available from: <http://authenticationworld.com/>
37. Professor Fred B. Schneider. CS 513 System Security -- Something You Know, Have, or Are [Internet]. [cited 2011 May 25]. Available from: <http://www.cs.cornell.edu/courses/cs513/2005fa/nnlauthpeople.html>
38. Biometrics.pdf [Internet]. [cited 2012 Jan 10]. Available from: http://citm.utdallas.edu/research/Publications/white_papers_source/Biometrics.pdf
39. Fritsch L, Fuglerud KS, Solheim I. Towards inclusive identity management. *Identity in the Information Society*. 2010 Oct 7;3(3):515–38.
40. Guidelines for Multimodal User Interface Design [Internet]. [cited 2012 Feb 20]. Available from: http://delivery.acm.org/10.1145/970000/962106/p57-reeves.pdf?ip=129.240.69.248&acc=ACTIVE%20SERVICE&CFID=85893110&CFTOKEN=75404391&__acm__=1329752112_1f0e26f3b4b106a336d55d51bc44aa01
41. Fuglerud KS, Reinertsen A, Fritsch L, Dale Ø. Universell utforming av IKT-baserte løsninger for registrering og autentisering. 2009 Jan 31 [cited 2012 Feb 16]; Available from: <http://publ.nr.no/4975>
42. FIDIS deliverable D7.2: Descriptive analysis and inventory of profiling practices: Future of IDentity in the Information Society [Internet]. 2005 [cited 2012 Apr 5]. Available from: <http://www.fidis.net/resources/deliverables/profiling/int-d72000/doc/2/>
43. WAI - Designing for Inclusion [Internet]. [cited 2011 Mar 20]. Available from: <http://www.w3.org/WAI/users/Overview.html>

44. Norges Blindeforbund. Fakta og publikasjoner [Internet]. [cited 2012 Apr 16]. Available from: <https://www.blindeforbundet.no/internett/fakta-og-publikasjoner>
45. Blindeforbundet. Internett [Internet]. [cited 2012 Apr 16]. Available from: <https://www.blindeforbundet.no/internett/tilgjengelighet/internett>
46. ETSI Technical Committee Human Factors (HF). Human Factors (HF); Multimodal interaction, communication and navigation guidelines. 2000;
47. What is assistive technology? [Internet]. [cited 2012 Feb 20]. Available from: <http://www.washington.edu/accessit/articles?109>
48. ACM Code of Ethics and Professional Conduct [Internet]. [cited 2012 Jan 10]. Available from: http://plone.acm.org/membership/COE_Flyer.pdf
49. Morville P, Rosenfeld L. Information Architecture for the World Wide Web: Designing Large-Scale Web Sites. Third ed. O'Reilly Media; 2006.
50. Universal Design Alliance (UDA): What is Universal Design (UD) - Seven Principles of Universal Design (Page 2 of 3) [Internet]. [cited 2011 Mar 20]. Available from: <http://www.universaldesign.org/universaldesign3.htm>
51. eInclusion | Europa - Information Society [Internet]. [cited 2011 Dec 2]. Available from: http://ec.europa.eu/information_society/activities/einclusion/index_en.htm
52. /d: LOV-2008-06-20-42 :d/ Lov om forbud mot diskriminering på grunn av nedsatt funksjonsevne (diskriminerings- og tilgjengelighetsloven) [Internet]. [cited 2012 Jan 9]. Available from: <http://www.lovdatabasen.no/all/tl-20080620-042-0.html#11>
53. Universell Utforming [Internet]. [cited 2011 Dec 1]. Available from: <http://universellutforming.difi.no/Hovudsider>
54. Colban A-M. Anti-Discrimination and Accessibility Act.
55. Denzin NK, Lincoln YS, editors. The SAGE Handbook of Qualitative Research. 3rd ed. Sage Publications, Inc; 2005.
56. Creswell JW. Qualitative inquiry and research design: choosing among five traditions. Sage Publications; 1998.
57. Using cultural probes for intranet user research » Step Two Designs, Patrick Kennedy [Internet]. [cited 2011 Nov 1]. Available from: http://www.steptwo.com.au/papers/kmc_intranetprobes/index.html
58. Pilot Study | Experiment-Resources.com | A website about the Scientific Method, Research and Experiments [Internet]. [cited 2012 Apr 5]. Available from: <http://www.experiment-resources.com/pilot-study.html>
59. About Tobii in Brief [Internet]. [cited 2012 Mar 27]. Available from: <http://www.tobii.com/en/eye-tracking-research/global/about-tobii/>
60. Moore RJ, Churchill EF. Computer Interaction Analysis: Toward an Empirical Approach

- to Understanding User Practice and Eye Gaze in GUI-Based Interaction. *Computer Supported Cooperative Work (CSCW)*. 2011 Sep 21;20(6):497–528.
61. e-Me [Internet]. [cited 2012 Jan 9]. Available from: <http://e-me.no/>
 62. Prototype [Internet]. [cited 2012 Apr 5]. Available from: <http://openid.e-me.no:8083/sample/InitTestPage>
 63. forskning.no > Lyd og bilder blir passord [Internet]. [cited 2012 Apr 16]. Available from: <http://www.forskning.no/artikler/2011/september/298908>
 64. Senter for IKT i utdanningen [Internet]. [cited 2011 Sep 30]. Available from: <http://iktsenteret.no/>
 65. Om Feide | Feide [Internet]. [cited 2011 Sep 23]. Available from: <http://www.feide.no/om-feide>
 66. Feide login to mobile apps | Feide [Internet]. [cited 2012 Apr 16]. Available from: <http://www.feide.no/feide-login-mobile-apps>
 67. TV2 Skole [Internet]. [cited 2012 Apr 16]. Available from: http://portal.tv2skole.no/Sider/om_oss.aspx
 68. Dahl M. Intervju with representant for Norwegian Center for ICT in Education. 2011.
 69. Marius Jørgenrud. Mobiltelefoner - Denne posen hindrer fjernsletting. [cited 2012 Apr 3]; Available from: <http://www.digi.no/893291/denne-poseden-hindrer-fjernsletting>
 70. Jonsson, E. Towards an integrated conceptual model of security and dependability [Internet]. 2006 [cited 2012 Mar 16]. Available from: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1625369>
 71. Weinschenk, Susan. The Secret to Designing an Intuitive UX | UX Magazine. 2010 Apr 8 [cited 2012 Apr 5]; Available from: <http://uxmag.com/articles/the-secret-to-designing-an-intuitive-user-experience>
 72. Mental Model Diagrams (Cartoon) | Smashing UX Design [Internet]. [cited 2012 Apr 25]. Available from: <http://uxdesign.smashingmagazine.com/2012/04/23/mental-model-diagrams-cartoon/>
 73. Apple - iOS 5 - See new features included in iOS 5. [Internet]. [cited 2012 May 2]. Available from: <http://www.apple.com/ios/features.html>
 74. Tobii_X60_X120_UserManual.pdf [Internet]. [cited 2012 Mar 6]. Available from: http://www.tobii.com/Global/Analysis/Downloads/User_Manuals_and_Guides/Tobii_X60_X120_UserManual.pdf
 75. Wroblewski L. Mobile First. 2011.
 76. Personas: bruk og praksis [Internet]. [cited 2012 Apr 23]. Available from: <http://personas.no/>

77. The Principles of Universal Design at Center for Universal Design [Internet]. [cited 2011 Dec 6]. Available from: <http://www.ncsu.edu/project/design-projects/udi/center-for-universal-design/the-principles-of-universal-design/>
78. Rømen D, Svanæs D. Validating WCAG versions 1.0 and 2.0 through usability testing with disabled users. *Universal Access in the Information Society* [Internet]. 2011 Sep 28 [cited 2012 May 1]; Available from: <http://www.springerlink.com/index/10.1007/s10209-011-0259-3>
79. Magne Lunde. Presentasjoner fra seminaret om brukertesting - Nyheter - MediaLT [Internet]. [cited 2011 Dec 6]. Available from: <http://medialt.no/news/presentasjoner-fra-seminaret-om-brukertesting/781.aspx>
80. W3C Multimodal Interaction Working Group [Internet]. [cited 2012 Apr 8]. Available from: <http://www.w3.org/2002/mmi/>

Appendix A

A list of all the services that are connected to Feide and that are available for the University of Oslo.

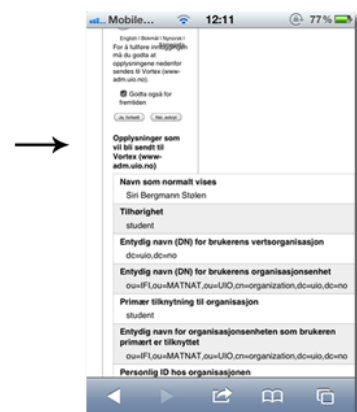
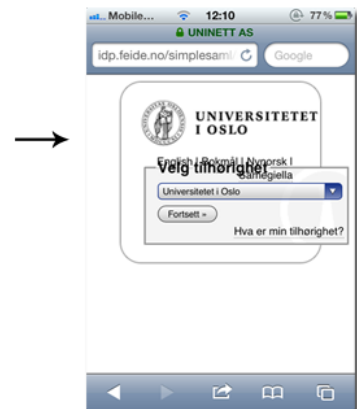
<ul style="list-style-type: none"> • Posten/Basware bestillingssystem for UiO • Lagring av elektronisk underlagsmateriale for vitenskapelig publikasjon • Cristin • NOTUR Plone autentisering • KUB - Den kunsthistoriske billed databasen • FAS integrasjon • Notur • Fasportalen • Posten/Basware bestillingssystem for UiO – KURS • Emner på Nett • Emner på Nett administrasjon • StudentWeb/SøknadsWeb • Metacenter administration system • Cloudstor@UiO • Fasportalens nødinnangang • FasServices • ePhorte • fsweb.no • Connect • TCS-eScience portal • Cloudstor 	<ul style="list-style-type: none"> • UNINETT Telefonkonferanse • EasyCruit E-Rekrutteringsløsning • Eduroam Debug Service • BIBSYS • Microsoft DreamSpark • Feide RnD • eValg ved Universitetet i Oslo • NB Digitalt Bibliotek • Bioportalen • UNINETT MailingLists Service • UiOs nettsted • Parkeringsoblat ved UiO • Studentlisens • Foodle • Jobbsøkersystem UiO • Wiki@UiO • StudentWeb/SøknadsWeb ved UiO • NRK Skole • WebID • viten.no • Creaza • eValg for UMB • UNINETT OpenWiki • UNINETT, Feide
--	---

Lars Kviteng (mail, 04.11.11)

Appendix B

Here is Feide login as it looks today, on desktop (in Firefox) and on a touch phone (in Safari/iPhone). The images shows login to the service Vortex provided by the University of Oslo.

Information that will be sent to Vortex (www-adm.uio.no)	
Display name
Affiliation	student
Distinguished name (DN) of person's home organization	dc=uiu,dc=no
Distinguished name (DN) of the person's home organizational unit	ou=IF ou=MATNAT,ou=UIO,cn=organization,dc=uiu,dc=no
Primary affiliation	student
Distinguished name (DN) of person's primary Organizational Unit	ou=IF ou=MATNAT,ou=UIO,cn=organization,dc=uiu,dc=no
Person's principal name at home organization@uiu.no
User ID



Appendix C


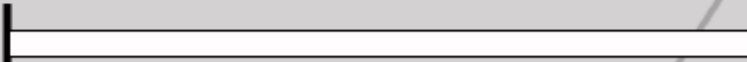

These are the probes that were used in the beginning of the data gathering.

Din Mobil

Personlig bruk

Har du skjermlås på mobilen din, i såfall hvilken?
(passord, pin etc.)

Hvor sikkert opplever du innholdet og tjenestene på din mobil?

veldig usikker
usikker
middels
sterk
veldig sterk

Foto


Kontekst

Hvor bruker du mobilen din?
Ta bilde av steder/situasjoner hvor du bruker mobilen din.

Forsøk å ta to/tre bilder hver dag. *(Du kan krysse av for bedre å holde oversikt over hvor mange bilder du har tatt.)*

Dag 1	Dag 2	Dag 3	Dag 4	Dag 5
<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

Sendes til: siribst@ifi.uio.no



Notater

Her kan du skrive ned andre kommentarer eller observasjoner.

Prosjektet

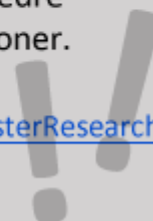
Autentisering, tilgjengelighet, smarttelefon

I forbindelse med min master i design, bruk og interaksjon ved UiO forsker jeg blant annet på hvordan våre forståelse av sikkerhet påvirker våre valg i forhold til innloggingsmekanismer.

Gjennom disse undersøkelsene håper jeg på å få bedre innsikt i dine relasjoner til sikkerhet på smart telefoner.

For mer informasjon se: <http://folk.uio.no/siribst/MasterResearch>

Takk for din deltakelse!



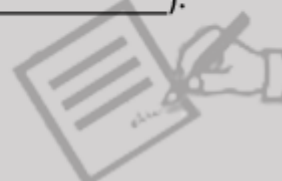
Samtykkeerklæring

Det bekreftes at innsamlet data vil bli behandlet anonymt og vil ikke bli gitt videre til en tredjepart.

Jeg samtykker med dette at:

- mine besvarelser kan medvirke til dette forskningsprosjektet
- jeg kan bli kontaktet for videre forskning senere i prosjektet. (via mail: _____).

Signatur: _____



Sikkerhet 2

Sikkerhet på mobil

Marker hvor sikker du opplever at din informasjon er når du benytter ulike autentiserings metoder.



Sikkerhet 1

Sikkerhet på datamaskinen

Marker hvor sikker du opplever at din informasjon er når du benytter ulike autentiserings metoder.



Spørsmål

Tre raske spørsmål

Noen uforutsette opplevelser ved bruk av mobil i dag, i såfall hva?

Hvor mange ganger har du brukt mobilen til å logge deg inn med?

Hva har du logget deg inn på i dag?

- Trådløst nettverk Applikasjoner Websider
 Telefon Simkort

Appendix D

Informed consent used for the interviews.

Samtykke

Masteroppgave – informatikk: design, bruk og interaksjon
Siri Bergmann Stølen

(tlf. 47339332, e-mail siribst@ifi.uio.no)

Prosjektbeskrivelse:

Prosjektet handler om tilgjengelig innlogging på touchtelefoner, men denne delen av forskningen ser først og fremst på hvordan mennesker tenker om sikkerhet på mobile enheter. Spørsmålene i dette intervjuet er basert på resultatene fra probene. Formålet med dette intervjuet er, i likhet med probene, å få bedre innsikt i folks forhold til sikkerhet og autentisering på smarttelefoner.

Intervju:

Deler av dette intervjuet vil bestå i å diskutere utfallet fra probene, for å bedre å forstå resultatene. Intervjuet er beregnet til å vare i ca. 30 min.

Du har sagt deg villig til å bli kontaktet etter å ha vært deltager i mitt probe prosjekt. All innsamlet data vil bli behandlet anonym, og din identitet vil ikke bli avslørt i noen rapporter som skrives fra intervjuet. Jeg vil ikke be deg om å oppgi sensitive detaljer under intervjuet. Du kan si så mye eller lite du ønsker og kan til en hver tid trekke deg fra intervjuet dersom du ønsker det. Intervjuet vil bli tatt opp, men opptaket vil ikke publiseres, og slettes dersom du velger å trekke deg. Opptaket og transkriberingen vil tilhøre prosjektet.

Det er ingen kjent risiko knyttet til deltagelse i dette studiet.

Dine fordeler:

Forhåpentligvis vil resultatene av dette studiet gagne samfunnet gjennom å gi større innsikt i mobil teknologi og menneskers interaksjon med denne.

Jeg godtar å delta i dette studiet:

Appendix E

The intervju guide that were used in the follow-up interviews with five students.

Intervju versjon 1

(Intervju av en uten skjermlås på telefonen)

- Gå gjennom agendaen (innledning, mobilbruk, datamaskin, litt om dine besvarelser, se på resultater fra probene og eksempler på autentiserings-mekanismer)

Innledning:

1. Hva heter du?
2. Hvor gammel er du?
3. Hva studerer du?
4. Hvordan er din bosituasjon (familie/kollektiv/alene)?
5. Hvilken smart telefon har du?

Mobilbruk:

1. På hvilken måte er du avhengig av telefonene din?
 - *Tar du med deg telefonen din uansett hvor du går?*
 - *Har du alltid oversikten over hvor telefonen din er?*
 - *oppbevarer du den i nærheten av deg til en hver tid?*
2. Hvilke applikasjoner med personlige opplysninger er tilgjengelig på din telefon?
 - *f.eks. Mail/kalender/nettbank*
3. Hvilke type informasjon som finnes på telefonene din ønsker du ikke at fremmede skal få tak i?
4. Du nevner at du har automatisk tilkobling til de fleste applikasjonene dine på telefonen (altså at du ikke trenger å taste innloggingsdetaljene hver gang du besøker applikasjonen), på hvilken måte er personvern avgjørende for deg når du velger å ikke logge ut av en applikasjon?
 - *Er det noen applikasjoner/tjenester hvor du ikke har automatisk innlogging?*
 - *Hvorfor/hvorfor ikke?*
5. Har du noen gang mistet eller blitt frastjålet telefonen din? Hva gjorde du da for å beskytte din info?

Datamaskin:

1. Hva tenker du om skjermlås på datamaskiner?
 - *På hvilken måte er det behov for dette?*

- *Er det noen situasjoner det er mer behov for det enn ellers? Hvilke?*
 - *Har du dette på din egen private datamaskin?*
1. På hvilken måte er personvern avgjørende for deg når du får spørsmål om du ønsker å lagre brukernavn og passord?
 - *Har du lagret passordene til tjenestene/websidene du bruker via datamaskinen?*
 - *Er det noen tjenester/websider du ikke lagrer passord på? Hvorfor/hvorfor ikke?*
 3. På hvilken måte skiller i informasjonene du oppbevarer på datamaskinen seg fra den informasjonen du oppbevarer på telefonen?
 - *Oppfatter du datamaskinen som sikrere enn telefonen, evt. Omvent?*
 - *Er det noe informasjon du kun ville oppbevart på en av enhetene?*
 4. Med tanke på innhold, tilganger etc., hva ville du vært mest redd for å miste, telefonen eller datamaskinen din?
 - *Hvorfor?*

Dine besvarelser:

1. Du har opplyst om at du ikke har noen skjermlås på din telefon, annet enn slideren. Hvis jeg spør om å få låne mobilen din, hva sier du da?
 - *Hvorfor? Hvorfor ikke?*
2. Hva er grunnen til at du ikke har skjermlås på telefonen din?
3. Har du tidligere hatt skjermlås på telefonen din? Hvis ja, hvorfor har du fjernet denne?

Nettskyen/the cloud:

1. Vet du hva som ligger i dette uttrykket?
2. I hvilken grad benytter du deg av nettskyen?
 - *Brukerdu f.eks. Dropbox.com, iCloud eller lignende tjenester?*
 - *Hvis ikke, hvorfor?*
3. Vet du hvem som har rettighetene til dine filer/opplysning som ligger lagret på nett?
4. Hvordan forholder du deg til autentisering på nettskyen sammenlignet med autentisering på din egen tlf. Eller datamaskin f.eks.?
5. Hvor sikker opplever du at din informasjon er når du lagrer den i nettskyen?

Tilslutt:

1. Kommer du nå til å opprette en skjermlås på telefonen din?
2. Har du noe du ønsker å tilføye helt til slutt?

Intervju versjon 2

(Intervju av en med skjermlås på telefonen)

- Gå gjennom agendaen (innledning, mobilbruk, datamaskin, litt om dine besvarelser, se på resultater fra probene og eksempler på autentiserings-mekanismer)

Innledning:

1. Hva heter du?
2. Hvor gammel er du?
3. Hva studerer du?
4. Hvordan er din bosituasjon (familie/kollektiv/alene)?
5. Hvilken smart telefon har du?

Mobilbruk:

1. I hvilken grad er du avhengig av telefonene din?
 - *Tar du med deg telefonen din uansett hvor du går?*
 - *Har du alltid oversikten over hvor telefonen din er?*
 - *oppbevarer du den i nærheten av deg til en hver tid?*
2. Hvilke applikasjoner med personlige opplysninger er tilgjengelig på din telefon?
 - *f.eks. Mail/kalender/nettbank*
3. Hvilke type informasjon som finnes på telefonene din ønsker du ikke at fremmede skal få tak i?
4. Du nevner at du har automatisk tilkobling til de fleste applikasjonene dine på telefonen (altså at du ikke trenger å taste innloggingsdetaljene hver gang du besøker applikasjonen), på hvilken måte er personvern avgjørende for deg når du velger å ikke logge ut av en applikasjon?
 - *Er det noen applikasjoner/tjenester hvor du ikke har automatisk innlogging?*
 - *Hvorfor/hvorfor ikke?*
5. Har du noen gang mistet eller blitt frastjålet telefonen din? Hva gjorde du da for å beskytte din info?

Dine besvarelser:

1. Du er en av dem som har opplyst om at du har skjermlås på telefonen din. Hva er grunnen til at du har dette?

2. Er det noen som kjenner ditt passord/pin/mønster?
 - *Hvordan har de fått greie på denne? Er du helt sikker på at det ikke er det? Hvorfor/hvorfor ikke?*
3. Føler du at din autentiserings mekanisme er trygg?
 - *Hvorfor/hvorfor ikke?*
4. Endrer du autentiserings mekanismen til telefonen din innimellom (hvorfor/hvorfor ikke)?
5. Hva skal til for at du skulle endret til en annen form for autentisering?
6. Hvis jeg fortalte deg at ditt passord/mønster/pin ikke var sikkert, ville du vurdert å endre det da?
7. Har du tidligere lat være å ha skjermlås på telefonen din? Hvorfor/hvorfor ikke?

Nettskyen/the cloud:

6. Vet du hva som ligger i dette uttrykket?
7. I hvilken grad benytter du deg av nettskyen?
 - *Brukerdu f.eks. Dropbox.com, iCloud eller lignende tjenester?*
 - *Hvis ikke, hvorfor?*
8. Vet du hvem som har rettighetene til dine filer/opplysning som ligger lagret på nett?
9. Hvordan forholder du deg til autentisering på nettskyen sammenlignet med autentisering på din egen tlf. Eller datamaskin f.eks.?
10. Hvor sikker opplever du at din informasjon er når du lagrer den i nettskyen?

Tilslutt:

1. Har du noe du ønsker å tilføye?

Appendix F

Testing of different password security meters shows that the result varies a lot based on which web site you are using.

Simple Form


First Name:

Last Name:

Company:

Email:

Password:



New password Strong

Verify password

Evaluate Your Password

Password: [Store](#)

Visibility: [Hide](#)

Before Redundancy Score: 49

Redundancy: 1.08

Significance Score: 0.00

Original Score: 9.8

Score: 9%


Complexity: **Very Weak**

Check your password—is it strong?

Your online accounts, computer files, and personal information are more secure when you use strong passwords to help protect them.

Test the strength of your passwords: Type a password into the box.

Password:

Strength:  Strong

Note: This does not guarantee the security of the password. This is for your personal reference only.

Test Your Password		Minimum Requirements
Password:	●●●●●●●●	<ul style="list-style-type: none"> • Minimum 8 characters in length • Contains 3/4 of the following items: <ul style="list-style-type: none"> - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	<input checked="" type="checkbox"/>	
Score:	84%	
Complexity:	Very Strong	

Passordstyrke: Sterk

Bruk minst åtte tegn. Ikke bruk et passord fra et annet nettsted, eller noe altfor opplagt, som navnet på kjæledyret ditt. [Hvorfor?](#)

Lag et passord

Bekreft passordet

Type the password:

Strength score is: Strength verdict:

Log:

- 12 points for length (13)
- 1 point for at least one lower case char
- 5 points for at least one special char
- 5 points for at least two special chars
- 2 combo points for letters, numbers and special chars

Hotmail address: @ hotmail.com

Create a password:
6-character minimum; case sensitive

Retype password:

Mobile phone: United States (+1)

Alternate email address:

Medium

Strong passwords contain 7-16 characters, do not include common words or names, and combine uppercase letters, lowercase letters, numbers, and symbols.

Appendix G

Informed consent used for the eye tracking.

Samtykke

Masteroppgave – informatikk: design, bruk og interaksjon
Siri Bergmann Stølen

(tlf. 47339332, e-mail siribst@ifi.uio.no)

Prosjektbeskrivelse:

Prosjektet handler om tilgjengelig innlogging på touchtelefoner, formålet med denne delen av forskningen er først og fremst å se på hvordan ulike autentiseringsmekanismer fungerer på touchtelefoner.

Eye tracking:

Denne testen vil bestå av to oppgaver etterfulgt av et par spørsmål. Hele sesjonen er beregnet til å vare i ca. 30 min.

Mens du utfører oppgavene vil dine øyebevegelser bli sporet og bli koblet sammen med video av skjermen på mobiltelefonen. All innsamlet data vil bli behandlet anonym, altså vil din identitet og dine autentiseringsopplysninger vil ikke bli avslørt i noen rapporter som skrives fra intervjuet. Du kan si så mye eller lite du ønsker og kan til en hver tid trekke deg fra intervjuet dersom du ønsker det. Intervjuet vil bli tatt opp, men opptaket vil ikke publiseres, og slettes dersom du velger å trekke deg.

Opptaket og transkriberingen vil tilhøre prosjektet.

Dine fordeler:

Forhåpentligvis vil resultatene av dette studiet gagne samfunnet gjennom å gi større innsikt i mobil teknologi og menneskers interaksjon med denne.

Jeg godtar å delta i dette studiet:

Appendix H

Eye tracking result from the user testing of the different authentication mechanisms in the e-Me prototype. Each color represents a users.

