UiO : Department of Informatics
University of Oslo

Exploring the Design of Authentication With Teenage Patients

Johan Sebergsen Steinberg

Master's Thesis Spring 2015

2015
Exploring the Design of Authentication With Teenage Patients
Johan S. Steinberg
http://www.duo.uio.no/
Print: Reprosentralen, University of Oslo

Abstract

Background Password and PIN based authentication does not longer fit in with how societies are expanding as Information Societies. The memory load they generate does not support the further digitalization of societies from new digital media, ubiquitous computing, and the expectation of citizens' digital participation from public and private sectors.

Objective The research interest of this study is to design a user-authentication method that is usable, accessible, and designed with and for teenage patients. This thesis will explore what a usable and accessible user-authentication method would be from the perspectives of long-term, teenage patients.

Methodology This study is located within the design methodology Participatory Design, and applies two qualitative design methods. The final prototype is based on the opinions of eight teenage patient participants from two design workshops.

Results The design process of this study ends with a suggestion for a user credential that would improve the Information Society by being usable, accessible, cool, and fun.

Conclusion I see two ways the design aspects that emerged in this project may influence society. First, it may re-establish user-authentication as a security measure for the end-users, and not a barrier. Secondly, it can contribute to how to further design accessible user-authentication.

Acknowledgments

I would most of all like to thank my supervisor, Maja, for guiding me through this combination of design, participatory design, teenage patients, research, and writing, but not by holding my hand (too much), but by helping me reflect a lot on my own. Thanks to Maggie, my co-supervisor, for your support and guidance. And a thanks to Jo, my other co-supervisor.

A very big thank you to all the patients who partook as co-designers in this project!

A thanks to my fellow students for great company throughout these two years. A special thanks to Simon, Trine, and Rebecca for good support and friendship.

Lastly, I would like to thank my family and all of my amazing friends outside of Blindern for your great support and for putting up with my confused head this past year (and in general)!

Johan S. Steinberg

Oslo, May 18, 2015

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Our everyday lives continues to become more digital — new digital devices, online banking, and web-based applications offering social connecting, social sharing, social networking, cloud storing, live collaborative editing, and the continuous transition to an electronic government (eGovernment) that increasingly applies web-based applications for the interaction with citizens. A person needs an online identity to get access and be able to use most of these applications. One form of online identity used by web-based applications is a user profile, created through a sign-up procedure. Later, when the person wishes to use the application, it must be confirmed that the person is really the user of the user profile. This is done through a process of logging in, where the person authenticates his/her identity with a user credential, e.g., a password. *Authentication*, or more precisely user-authentication or human-by-machine authentication (as opposed to machine-by-machine authentication), can be defined as the whole process of verifying the validity of a claimed user [56]. In this thesis 'authentication' refers to the whole process of user-authentication if not otherwise stated.

On the Web, password based authentication is still the dominating authentication method. In the days before password requirements, a password could be a simple, memorable word. Now, computers are able to guess "an astounding 8.2 billion password combinations each second" [26]. Thus, to make passwords more secure, users are required to create and use passwords that are are difficult to guess by using non-dictionary words, by being over a certain length, by including numbers, special characters, or capital letters. Users are also recommended not to use the same password everywhere, users should regularly change passwords, and sometimes they are forced to change them. In this digital society, passwords are not as simple as Ali Baba's 'open sesame'[1] anymore. Passwords are often needed and often forgotten.

With societies' increasing reliance on the services enabled by the Internet — authentication plays a key role in the inclusion or exclusion of people in the *Information Society*. The next section will further expand on the background of this thesis.

1.1 Background: In an Information Society

Information and communications technology (ICT) is no longer a supporting function, but rather the core of the operation. ICT fundamentally transforms how goods and services are supplied. "Many industries, such as banking and travel, have understood and used ICT innovatively to give customers better, faster services and to improve the efficiency of their internal processes" [52]. In Norway, many public sector services are already digitized, and the Government wants to increase the pace of public sector digitalization [52]. "Norway is to be at the forefront internationally in terms of providing digital public services to its citizens and businesses" [23]. The agenda for Norway's future public sector is to be accessible online to the extent possible, and web-based services are the general rule for communication with citizens, organizations and businesses [23, 52]. Submission of applications, invoicing, making appointments, and distributions of decisions and various types of reports are to be done via digital communication [23]. The Norwegian Government also has a goal to digitize Norway's business sector as much as possible [52].

While governments are becoming more digital, other parts of society have lead the way in the transition to an Information Society. People have never had easier access to information, or more ways to communicate with one another than now. Face-to-face communication is partly and increasingly coexisting with communication via the combined effort of the Internet and smart devices. Baym sums up the change of communication as follows:

> "Once limited to face to face conversation, over the last several millennia we have steadily developed new technologies for interaction. The digital age is distinguished by

[1] In the folk tale 'Ali Baba and the Forty Thieves', Ali Baba opens the secret thieves' den with the passphrase 'open sesame' [3].

> rapid transformations in the kinds of technological mediation through which we encounter one another. Face to face conversation, landline telephone calls, and postal mail have been joined by email, mobile phone calls, text messaging, instant messaging, chat, web boards, social networks, photo sharing, video sharing, multiplayer gaming, and more." [6, p. 1]

New media is changing the nature of how people connect socially. *Social media* have been defined by Kaplan and Haenlein as "a group of Internet-based applications that build on the ideological and technological foundations of Web 2.0[2], and that allow the creation and exchange of User Generated Content" (as cited in [60, p. 173]). "Social media have revolutionized the communication landscape, becoming an integral part of how we communicate" [60, p. 175]. Another part of the revolution lays in what is called *ubiquitous computing* or *pervasive computing*; a state of computing and networking in society that appears to be everywhere seamlessly [68, 81]. Interaction with digital media happens from laptops, smart devices, hand-held devices and wearable devices; for getting information, sharing content, and generally being social and interacting with society. The mobility enabled by these digital devices and its relations with the new digital media has further changed the landscape of social interaction. Thus, a big, expanding part of society takes place digitally. The words of the Norwegian Ministry of Local Government and Modernisation then applies to society for the public and privat sector, and at a personal level: "A growing number of areas in Norwegian society are based on the premise that its citizens are online. Consequently, if you are not online, you will often feel excluded from society" [52].

1.1.1 An Information Society for All

The Norwegian Government regards digital participation from all citizens crucial to ensure that ICT contributes to value creation and growth in society [52]. The white paper *An Information Society for All* presents three preconditions for how everyone will be able to digitally participate in Norway: digital access, digital competence, and Universal Design of ICT [51]. 'Digital access' concerns access to ICT, and focuses mainly on

[2] Web 2.0 suggests a new version of the World Wide Web that "emphasize user-generated content, usability, and interoperability" [80]. The term was first used in 1999 [80].

how all citizens should have broadband access [51]. ‘Digital competence’ concerns reaching a societally acceptable level of knowledge on ICT, and focuses mainly on the required education in school [51].

Universal Design

To not be excluded from the Information Society, there is need for more than digital access and digital competence. ICT must be designed correctly. *Universal Design* (UD) is the only design approach the Norwegian Government names as a precondition for an ‘Information Society for all’. UD’s responsibility in this context is to guide how ICT is accessibly designed. *Accessibility* in Human Computer Interaction (HCI) is especially concerned about access for the groups of people in society that require any kind of special consideration to be able to use technology [7]. These groups may be elderly, children, and people with disabilities or that are vulnerable in other ways. In detail, these people include:

- Physically people that “can be excluded because of inappropriate siting of equipment or through input and output devices making excessive demands on their abilities. For example, an ATM may be positioned too high for a person in a wheelchair to reach, a mouse may be too big for a child’s hand or a mobile phone may be too fiddly for someone with arthritis to use” [7, p. 80].
- Conceptually people that “may be excluded because they cannot understand complicated instructions or obscure commands or they cannot form a clear mental model[3] of the system” [7, p. 80].
- Economically people that “are excluded if they cannot afford some essential technology” [7, p. 81].
- People that are culturally excluded as a result of “designers making inappropriate assumptions about how people work and organize their lives. For example, using a metaphor based on American football would excluded those who do not understand the game” [7, p. 81].
- People that are socially excluded “if equipment is unavailable at an appropriate time and place or if people are not members of a particular social group and cannot understand particular social mores or messages” [7, p. 81].

[3] A person’s mental model represents how a person understands and knows something [7].

By defining accessible ICT as aiming to include the above user-groups, the concept of accessibility is reaching wider than UD. Specifically with regards to the economical aspect, which falls under 'digital access' in the white paper *An Information Society for All* [51].

According to Benktzon the typical model in UD is a user-pyramid, as illustrated in Figure 1.1, "where the lower portion are the able-bodied or fully capable users together with elderly people who have minor disabilities such as reduced strength or impaired hearing or sight. In the middle of the pyramid are people with reduced strength and mobility caused by disease and more severe, age-related impairments. This group contains many older people. At the top of the pyramid are those severely disabled people who need help with many daily activities: people in wheelchairs and people with very limited strength and mobility in their hands and arms" (as cited in [20, p. 66]).

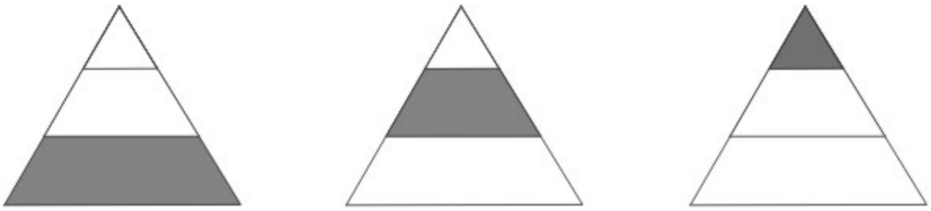


Figure 1.1 The user pyramid of Universal Design — three levels where the top represents the few, severely disabled people (as depicted by Dong in [20]).

Assistive technology — technology that is purpose-built for people with disabilities — has a top-down approach to designing for accessibility [20]. The UD approach distinguishes itself from assistive technology by having a focus on how something in its basic design should aim to include as many user groups as reasonably possible, not necessarily by creating additional assistive technology [20]. This will better ensure that vulnerable users are not an 'after thought' in design of ICT. According to Dong, UD has gone through paradigm shifts, moving towards what he calls an Integrated Universal Design Approach where the paradigm has shifted to the integration of the 'bottom-up' and 'top-down' approach" [20].

For physical spaces in Western countries, there are generally legal and ethical requirements of access for people with disabilities. Many information spaces are also obliged to comply [7], also in Norway with a regulation that states that ICT should incorporate principles from UD [2, 51]. Simplified, the Agency for Public Management and eGovernment describes UD as designing, or accommodating something so as many people as possible can use it, regardless of disabilities [2]. The principles of universal design, which defines how something in general can be universally design [7], does not only concern accessibility, but also usability. Good usability in HCI is normally focused on efficiency, effectiveness, ease of learning, safety in use, and high utility [7] and the universal design principles cross over to this focus. The principles of universal design are:

> "*equitable use* — that the design does not disadvantage or stigmatize any group of users; *flexibility in use* — that the design accommodates a wide range of individual preferences and abilities; *simple, intuitive use* — the use of the design should be easy to understand regardless of the user's experience, knowledge, language skills, or current concentration level; *perceptible information* — that the design communicates necessary information effectively to the user, regardless of ambient conditions or the user's sensory abilities; *tolerance for error* — that the design minimizes hazards and the adverse consequences of accidental or unintended actions; *low physical effort* — that the design can be used efficiently and comfortably, and with a minimum of fatigue; *size and space for approach and use* — that the appropriate size and space are provided for approach, reach, manipulation, and use, regardless of the user's body size, posture, or mobility."
> (as cited in [7, p. 81])

The requirements of how UD is regulated in Norway are much simpler; UD of ICT is regulated by following established and standardized guidelines [2]. Websites are required to follow the Web Content Accessibility Guidelines (WCAG) 2.0 to what is called an AA level, of all together three levels: A, AA, and AAA [2].

1.1.2 User-Authentication

Since online identities can include a lot of personal information user-authentication is security, and sometimes referred to as the first line of defense [81]. Todorov defines authentication as follows:

> "The process of Authentication is often considered to consist of two distinct phases: (1) identification and (2) (actual) authentication.

> *Identification* provides user identity to the security system. This identity is typically provided in the form of a user ID. [. . .]
>
> *Authentication* is the process of validating user identity. The fact that the user claims to be represented by a specific abstract object (identified by its user ID) does not necessarily mean that this is true. To ascertain that an actual user can be mapped to a specific abstract user object in the system, and therefore be granted user rights and permissions specific to the abstract user object, the user must provide evidence to prove his identity to the system. Authentication is the process of ascertaining claimed user identity by verifying user-provided evidence." [72, p. 5]

In general, a person needs an online identity to get access and be able to use web-based applications. To get and use an online identity, it must be confirmed that the online identity really belongs to the person. When authenticating, a person provides evidence to confirm the validity of his/her identity. The evidence is the *user credential(s)* and it incorporates the *authentication factor(s)* of an authentication method. Basically, there are three categories of authentication factors [46, 49, 56, 72]:

- *What you have*, or object-based authentication, e.g., a token or a key.
- *What you know*, or knowledge-based authentication, e.g., a password or PIN (personal identification number).
- *What you are*, or ID-based authentication such as a measurable biological or behavioral characteristic that reliably distinguishes one person from another, i.e., a biometric factor, or traditionally a photo ID.

These factors are often multiplied or combined to increase security. O'Gorman gives a good description of how the level of security works in computer security. It is as follows:

> "Security systems and methods are often described as strong or weak. When used in relative terms, the meanings are clear. A door with a lock offers stronger security than one with no lock. A credit card number alone offers 'weak' defense

> against repudiation because a user can easily deny a credit card charge by claiming that his credit card number was stolen. However, a credit card number plus a signature has a 'strong' defense (meaning 'stronger' defense than without a signature) because the user leaves evidence of his presence by his signature." [56, pp. 2022-2023]

Use Issues

For what can be considered the most popular authentication methods — password based, PIN based, and fingerprint based — there are not many studies on their effect on people with disabilities. Helkala "discusses the potential impact of Parkinson's disease, dyslexia, vision impairment, and upper extremity disabilities on the security level and usability of PIN codes and textual passwords. Through the discussion, the author highlights different challenges of each condition and suggests that the authentication problem for people with disabilities needs to be addressed by studying constituent groups and categories separately" (as cited in [46, p. 4]). Feng et al. found that children and young adults with Downs Syndrome had difficulty remembering passwords and often relied on a third party to enter passwords on their behalf (as cited in [46]). Some children and young adults with Downs Syndrome did not understand why the mechanism was needed or how it worked, resulting in more instances of sharing passwords with others (as cited in [46]). Another study by Kumin et al. found that adults with Downs Syndrome often stored their passwords on their home or work computer, so that they didn't need to remember them. "For these users, some forms of security and privacy protection mechanisms end up being a key interaction barrier" (as cited in [46, p. 4]).

On a general level, password-use for any user may be moving towards unacceptable amounts of "*memory load*" [79]. The growth of the Information Society has made memory-load problems of passwords more evident. Users must generate multiple passwords satisfying different criteria for a variety of websites. For example, some websites have no restrictions on a user's password, whereas others require a minimum length, a mixture of letters and digits, and so on. Some sites additionally require special characters in the password, whereas others do not allow use of special characters. Neath explains how the ability to retrieve items in memory is dependent on memory load: "As memory load increases, the number of forgotten items increases" (as cited in [79, p. 754]). Most people may be able to remember a few unique passwords, but as the number of passwords that a user has to remember increases, the likelihood of recalling a specific password decreases. The often repeated 'solve everything' tip by news media is to use a password manager that can store and create passwords for you [58], but the prerequisite, technical know-how needed across several devices and operating systems is often forgotten by news media. For some user-groups, password managers are 'unaccessible' from the complex mental models they create. *Mental models* are "the models people have of themselves, others, the environment, and the things with which they interact. People form mental models through experience, training, and instruction" [54, p. 17].

On the phone, PIN based authentication has been thriving. PINs are classically used with payment cards, and have also been adopted by smart cards that can be used as a credential at some sites that require higher security [15]. In the paper "The Coming PIN Code Epidemic," Rasmussen and Rudmin describes the situation as follows: "Most people must remember various numeric passwords, security codes and PIN numbers for banking, credit cards, debit cards, online accounts, mobile phones, door locks, luggage locks, etc." [61, p. 5]. PIN based authentication, as password based authentication, authenticates by being a secret only the user knows and thus face some of the same problems as the password. The memory load from the amount of PIN numbers may be an issue for users [61], in particular when people are not allowed to choose their own PIN code, or when PIN codes change, e.g., upon receiving a new payment card.

For the commercial product the 'iPhone 5S', fingerprint based authentication technology was introduced. In a popular technological consumer product, it may be a breath of fresh air as a serious challenger in an area where password and PIN based authentication have dominated. However, some issues are dawning. With an increasingly online and connected world, the uniqueness of fingerprints have been questioned, and for people working with their hands, false negative authentication results are common [40, 50]. Jain et al. further explains that fingerprints of a small fraction of the population may be unsuitable "because of genetic factors, aging, environmental, or occupational reasons (e.g., manual workers may have a large number of cuts and bruises on their fingerprints that keep changing)" [33, p. 126]. Because of a high number of false negatives of current fingerprint technology, it is still dependent on a fallback that uses a PIN/password. The solution on the Iphone is also known to be *hackable* [82]. In computer security, a hacker is someone who seeks and exploits weaknesses in a computer system or computer network [27]. The fingerprint based authentication on the Iphone can mainly be considered a practicality for the user, not a security [39].

Password based authentication is dominating the Web, and from how so many applications — for any device — are web-based, there is no escaping passwords. The authentication methods smart devices and computers apply, will in several situations come as a pre-authentication in addition to the authentication required by many web-based applications.

Consequences of the Use Issues

Users with disabilities are continuously confronted with barriers to use everyday ICT. Similarly to how user-authentication is called the first line of defense [81], it is also often the first barrier to use ICT. But it is not only a barrier for people with disabilities. According to Norman, password based authentication is a classic example of how, when "[t]he more secure you make something, the less secure it becomes" [55, p. 60]. Everyday security is circumvented by people, for example by doors propped open by bricks and wastebaskets, and "house keys under the door mat, above the door frame, or under fake rocks that can be purchased for this purpose" [55, p. 60]. Similarly, password based authentication is also circumvented. Because of different recommendations and requirements, each new password makes every password more difficult to remember. Passwords are pasted on the front of monitors, hidden under keyboards or in drawers, and passwords such as 'abc123', 'qwerty' and 'password' have been at the top of the list of the most used passwords for several years [1]. A survey of 3050 Web users conducted by Rainbow Technologies found that 55% of the respondents admitted to writing down at least one password, with 8% indicating that they wrote down all of their passwords (as cited in [79]). In a follow-up to the Rainbow Technologies survey conducted by SafeNet, 50% indicated having written down at least one password, and 10% said that they always wrote down their passwords (as cited in [79]). For the fingerprint based authentication on the Iphone, sites have recommended users to scan the same finger from several different angles to decrease the false negative rate [70, 73]. In the words of Norman: "[. . .] when security gets in the way, sensible, well-meaning, dedicated people develop hacks and workarounds to defeat it" [55, p. 60].

Users' circumvention of security is also blamed on how users do not have enough understanding of security procedures, and how sufficient training must be provided [22]. But some actors still do not think that the design or training can be blamed, only the users. On the front page of Norwegian newspaper Dagens Næringsliv from May 8, 2015, lawyer Christian Sturla Svensen goes out and says he thinks employees should be fired for breaking security routines, e.g., for writing down passwords on a note, he says [22].

Consequences of Authentication's Role in Society

A wide range of theoretical perspectives try to explain the ways that technology and society are linked, each of them shedding light on different aspects of technological society [60]. Feenberg has developed a theoretical model to examine the theories of technology and society, in which he distinguishes between two central dimensions: (1) neutral versus value-laden, and (2) autonomous versus human controlled (as cited in [60, p. 43]). In relation to the first dimension, Verbeek argues how technology has values based on how artifacts mediates:

> "Telephones mediate the way we communicate with others, cars help to determine the acceptable distance from home to work, thermometers co-shape our experience of health and disease, and antenatal diagnostic technologies generate difficult questions regarding pregnancy and abortion. [. . .] the conclusion seems justified that artifacts have morality: technologies play an active role in moral action and decision-making." [77, p. 93]

Verbeek asks how technology's morale can be understood? Can artifacts be considered moral agents [77]? "In order to be held morally accountable for an action, an agent needs to have the intention to act in a specific way, and the freedom to realize this intention" [77, p. 93]. In order to explain the intentionality of technology, Verbeek makes a distinction between two aspects of 'intentionality': (1) the ability to form intentions, and (2) the spontaneousness of forming intentions [77]. Strictly speaking, Verbeek sees no such thing as 'technological intentionality', but he sees artifacts as active in shaping human actions, interpretations, and decisions; actions, interpretations, and decisions that would have been different without the artifact [77]. For the first aspect of intentionality, technological artifacts do not deliberately do something, but have intentions "found in their directing role in the actions and experiences of human beings" [77, p. 95]. For the second aspect of intentionality, since artifacts can only play their ‘intending’ mediating roles within the relations between human beings and reality, the subjects who act or make decisions about actions are never purely human, but rather a complex blend of humanity and technology [77]. “[I]ntentionality comes about in associations between humans and nonhumans. For that reason, it could be called ‘hybrid intentionality’, or ‘distributed intentionality’” [77, p. 96].

For the first dimension of Feenberg’s model (as cited in [60]), Verbeek argues for value-laden artifacts by explaining how they direct peoples actions, intentions, and decisions [77]. For the second dimension — if artifact have autonomy or are human controlled — can we say that technological artifacts have freedom? [77]. Obviously not, he says, but they are a part of the environment in which human existence takes place and takes its form [77]. And like intentionality, he sees freedom as a hybrid affair [77]. Verbeek does, however, exclude technological artifacts themselves from having freedom — by defining ‘freedom’ as not to be understood as the absence of ‘external’ influences on agents, but as the practice of dealing with such influences or mediations [77, p. 99].

In 1986, Langdon Winner analyzed a number of ‘racist’ overpasses in New York, which were deliberately built so low that only cars, not buses, could pass beneath them, thus preventing the dark-skinned population, unable to afford a car, from accessing the beach (as cited in [77, p. 92]). The important role of authentication as a gateway in the Information Society, combined with interaction design issues, makes authentication discriminate people. As the ‘racist’ overpasses, authentication is not neutral in its societal context. Opposed to the overpasses, authentication is (most likely) not deliberately designed inaccessible, but when it is inaccessible it may have an even greater consequence than the overpasses. An excluded person will lose normalized ways of communicating within society, which leads to a loss of freedom and independence. For the second dimension of Feenberg’s model, authentication as a gateway is not autonomous. As freedom can be defined as the “practice of *dealing* with such influences or mediations” [77, p. 99], but the design of it must be regulated.

1.2 Designing for KULU

An authentication method is a security mechanism, and security have tended to focus more on the security than the user. Some claim that usability is still a poorly understood element of computer security [35] (for authentication it is perhaps also neglected; passwords are partly dominant because of its low cost [29]), and perhaps the entire convenience of use that interaction design can provide is neglected, as O'Gorman unintentionally gives a clue of in his paper "Comparing passwords, tokens, and biometrics for user authentication," claiming that the factor of user convenience is relatively straightforward:

> "Comparison factors [for human authenticators] are security, convenience, and cost. The latter two factors are relatively straightforward [. . .]; however, security as measured by vulnerability to applicable attacks is not so straightforward [. . .]" [56, p. 2022]

This project focuses on the human side of user-authentication, and the issues of the user interaction that can have increasingly negative consequences for citizens and societies. A user-group with special needs when it comes to sensitive personal data, and possibly also with personal experiences and contemplation on user-exclusion, are long-term, teenage patients. Based on their technological understanding and their youth, the 'teenager' user-group is also an important group regarding the use of technology for the modern world.

This project is part of a research project called KULU, based at the Design group of Department of Informatics at the University of Oslo. KULU is about cool technology for young people with long-term or chronic health challenges. "We [KULU] want to understand how young patients use online resources and we design interactive technologies that support them in their autonomy, both as young people and as patients" [42]. *Participatory Design* (PD) is often applied as a design methodology in KULU related projects. With a focus on participation in the design process to understand and 'hear' the future users of a design, PD has a strong ethical focus at its core. PD's ground principles supports this by focusing on power relations, giving the weaker a voice, democratic practices, and designing with participants in a two-way learning situation, often in the situational context of what that is to be designed [38]. KULU focuses on having participants and co-designers in the design process to actually be long-term, teenage patients. These patients have a diverse range of health challenges

In a society where authentication happens every day, many times a day, it seems obvious that the current state of password and PIN based authentication is inconsiderate of conceptually vulnerable users.

With the growing Information Society, this state of user-authentication will soon not be usable for any user group as all human beings have conceptual limitation. Fingerprint based authentication is still not a complete solution — if it ever will be. Therefore I see it as important for the future of the Information Society to study and contribute to cleaning up the mess that is user-authentication.

1.3 Research Interest

Universal Design (UD) aims to design, or accommodate, something so as many people as possible can use it, regardless of disabilities [2]. UD can be said to have evolved into an integrated design approach for accessible ICT [20]. As an effect, 'universally designed' technology is increasingly overlapping with technology designed with the top-down assistive technology approach, and can replace certain assistive technologies. UD is a precondition for the Norwegian 'Information Society for all' [51], and perhaps it is so because it has evolved to an integrated approach, making it suitable for user-inclusion of many diverse user groups. By becoming an integrated approach and because it is a chosen precondition for user inclusion in Norway, the UD approach today has an increasing responsibility of supporting user-inclusion.

In Norway, ICT must by law be 'universally designed' by following standardized guidelines [2]. For password based authentication implementation on the Web, the implications of these regulations are to follow WCAG 2.0 to a level of AA. However, WCAG 2.0 can at best fix the surrounding Web 2.0 elements of an authentication method, not the issues related to the user credential of password based authentication. To design a universal authentication method, it is necessary to look further than standardized guidelines. Security 'gets in the way' and people often want to exclude intrusive security measures from their daily life by circumventing them. Is it possible for a security design to not make users do that? If it is, the only way to find out is by including the users themselves in the design process as co-designers. Hence, I have formulated my main research interest as a design aim:

> "To design a user-authentication method that is usable, accessible, and designed with and for teenage patients."

This thesis will explore what a usable and accessible user-authentication method would be from the perspectives of the teenage patients that are participating in KULU. This thesis further aims to include their say in the discussion of the future universal user-authentication method that is better suited for the digital expansion of the society.

1.3.1 Related Research

There hardly seems to exist any studies that studied user-authentication designed with patients, teenagers or just with the future users themselves. For a study, published in 2009, Riley et al. used Participatory Design (PD) to design a graphical user interface for a fingerprint system [64]. Two workshops were held with all together 82 participants in the ages between 18 to 62. In the first workshop, participants made low fidelity paper prototype of improvements to already existing fingerprint system interfaces. The participants focused on better instructions for using the system. Both instructions for finger placement and an instructional video were included in a prototype that was user evaluated in the next workshop. Here, the participants found the technology easy to use, and the main conclusion was that the way feedback is presented effects overall system performance. The design process ended with a high fidelity prototype based on both workshops. In a final questionnaire, when answering a question about the privacy impact of this system, some participants were concerned (without further information). Riley et al. believes that the adoption of biometric based systems like this are slow because users doubt their security [64].

In a paper by Clement et al., published in 2012, they sought to see how PD inspired design interventions could open up possibilities for infrastructural reform on jurisdictional identity schemes [16]. Clement et al. executed a series of PD-inspired interventions into the public policy discussion with a "modest goal of opening a public discussion about the many issues it [Enhanced Drivers Licenses] raised and the prospect of privacy protective alternatives" [16, p. 21]. "Drawing on 'classic' PD precepts, such as iteration, realistic use scenarios, ethnographically informed fieldwork, situated reflection, and mock-ups and prototypes", they experimented publicly with various artifacts that range from a mock radio frequency ID (RFID) scheme to an Android phone digital ID wallet application [16, p. 21]. According to Clement et al., based on the feedback from the public, it "did seem to help people connect their life experiences with infrastructures, or to imagine the impact an infrastructure change might have on their own activities. Our data for this is largely anecdotal, however; a potential ongoing challenge to designing alternative infrastructures is assessing the result of the intervention" [16, p. 29].

There is a lack of studies that focus on how the users themselves would like user-authentication to be designed, and especially to a degree where the users are so involved that they can be considered co-designers.

1.4 Chapter Guide

Chapter 2

Methodology

This chapter will present *Participatory Design* (PD) — the design methodology used in this project — and the two design methods that were applied for two different workshops. The methods for this project were qualitative.

2.1 Participatory Design

"Participatory Design is a design methodology in which the future users of a design participate as co-designers in the design process" [76, p. 1] — this participation lasts throughout the design process [65, 66]. Robertson and Simonsen defines the essence of PD as the following:

> "a process of investigating, understanding, reflecting upon, establishing, developing, and supporting mutual learning between multiple participants in collective 'reflection-in-action'. The participants typically undertake the two principal roles of users and designers where the designers strive to learn the realities of the users' situation while the users strive to articulate their desired aims and learn appropriate technological mean to obtain them." [65, p. 2]

PD was pioneered in Europe and especially Scandinavia in the 1970s [65]. It was a response to the transformation of workplaces driven by the introduction of computers [65]. Some of the early 'seeds' of PD were cases involving trade union activists seeking to influence the fast-paced emergence of automation at their workplaces, and ethnographic studies about the introduction of technology into workplaces [38]. Sanders and Stappers sums up their opinion of why they think PD is still, and increasingly being considered an important design practice: “Over the past six decades, designers have been moving increasingly closer to the future users of what they design. Especially in areas where technologies mature, and the next new feature is no longer of value, manufacturing companies have been increasingly open to approaches that define the product based on what people need” [66, p. 6]. The need for participation is according to Kensing and Greenbaum based on several arguments: “One, a political argument, emphasises that people *should have the right* to influence their working conditions. Another central arguments is pragmatic. Its focus is that in the process of involving people who will be affected as active participants, learning will take place between the ‘experts’ and the participants which can result in better designs” [38, p. 27].

2.1.1 Core Perspectives

“PD is not defined by formulas, rules and strict definitions but by a commitment to core principles of participation in design” [65, p. 3]. Based on its basic world view that is concerned about the fact that IT is never neutral, the core perspectives of PD are ‘having a say’, ‘mutual learning’, and ‘co-realization’ [12]. The core perspectives are all connected and influence each other.

Having a say in the design process basically means having influence over the design outcome. Besides that the users need to be involved in the design process, Bratteteig et al. specifies that “[t]o have an influence implies that the users need to be informed, they need to be given the chance to form and express their opinion, and they need to be given the power to influence the decisions in design” [12, p. 129]. This implies that a fundamental principle in PD — “the sharing of decision-making power between all participants in the design process” — is addressed by ‘having a say’ [12, p. 129].

The second perspective, *mutual learning*, is about mutual respect. Mutual learning is important because that is how mutual respect between different groups is achieved. For the users to trust the designers and their visions, they have to get “to know and respect each other across differences in position, perspective, knowledge and skills” [12, p. 132]. Mutual learning is always two-way learning. It is grounded in the fact that the users know most about the domain and use context of the design to be, and the designers know about the design process and technical issues [12].

The last perspective is *co-realization*. It is the creation of involvement in design [12]. Prototyping is seen as the most important method for visualizing possible solutions — "to enable co-construction and learning through sharing concrete experiences of a new imagined artefact" [12, p. 133]. Co-realization also involves the intertwining of analysis and design. PD tries to actively involve users in the analysis of design, making it "an activity of exploring opportunities for change" [12, p. 135].

2.1.2 Design Process

Historically PD has had several ways to carry out its methodological whole. PD as a methodology can be understood as "a coherent set of organizing principles and general guidelines for how to carry out a design process from start to finish [. . .] guidelines that must be carefully selected, adapted and appropriated to the specific project and situation at hand" [12, p. 118]. This project takes the methodological approach of 'use-oriented design'. Here, the design process follows an iterative cycle of six activities where each activity can utilize the necessary methods and tools best suited for its aim [12] (see Figure 2.1). Use-oriented design is grounded in future use, and is concerned with activities, and the logic of activities rather than the users, but, however, "use is only accessible through users" [12, p. 126]. "The approach is explorative, aiming to postpone the decision about the design problem so that users and designers can collaborate (or negotiate) on the problem setting after they have got to know each other" [12, p. 127].

Use-oriented design emphasizes the early stages of the design process, ending "up with a stepwise refining of a prototype to an unambiguous specification for a system" [12, p. 127]. Sanders and Stappers describes the early stages of the design process as the 'fuzzy' front end: "The front end describes the many activities that take place in order to inform and inspire the exploration of open-ended questions [. . .] The front end is often referred to as 'fuzzy' because of the ambiguity and chaotic nature that characterise it" [66, p. 7]. What follows the front end, according to Sanders and Stappers, is a more traditional design process "where the resulting ideas for product, service, interface, etc., are developed first into concepts, and then into prototypes that are refined on the basis of the feedback of future users" [66, p. 7], see Figure 2.2. Sanders and Stappers' figure shares relations with two terms of design thinking: *divergent* and *convergent*. The design process starts divergent by covering broader issue, finding more alternatives, and exploring more opportunities [44], and the process ends convergent by focusing more

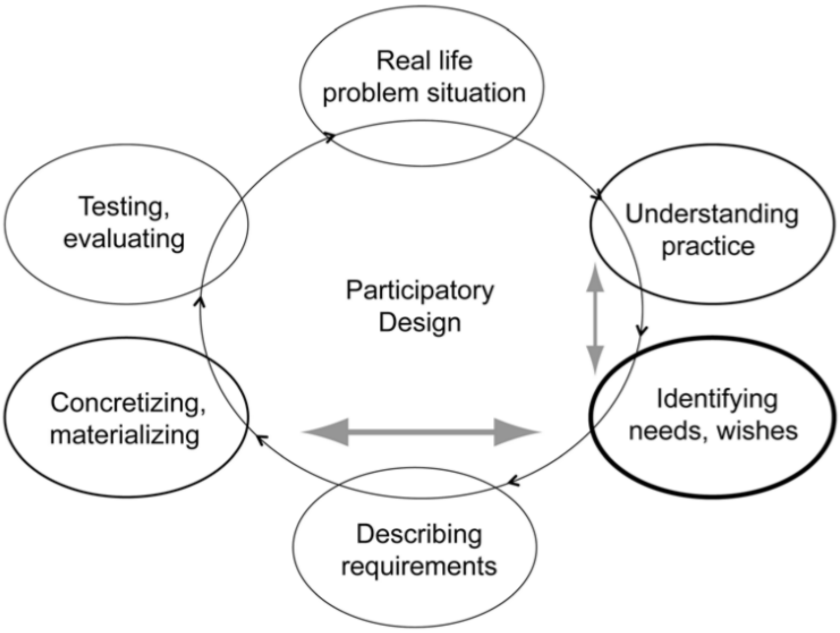


Figure 2.1 The design cycle when following a use-oriented approach within PD (as depicted by Bratteteig et al. [12]).

on a specific solution "or a synthesis of several ideas" [44, p. 29].

In the design process the participants have the roles of 'expert of his/her experience', and plays a large role in knowledge development, idea generation and concept development [66]. The researcher and designer (which may be the same person) "supports the 'expert of his/her experience' by providing tools for ideation and expression" — s/he is a facilitator [66, p. 12].

2.2 Methods

Two methods were chosen for the design process of this thesis: Future Workshop and Experience Prototyping. According to Brandt et al., methods does not have to be applied rigorously and by the book, instead they suggest to use methods so that they support "participants in the making, telling and enacting aspects of future design" [11, p. 146]. Figure 2.3 shows the tell-make-enact diagram to remind us that tools and methods do not operate in isolation [11, p. 149]. *Methods* explains how specific activities are carried out, while *tools* are instruments that supports the methods. The arrows in the diagram are double-headed

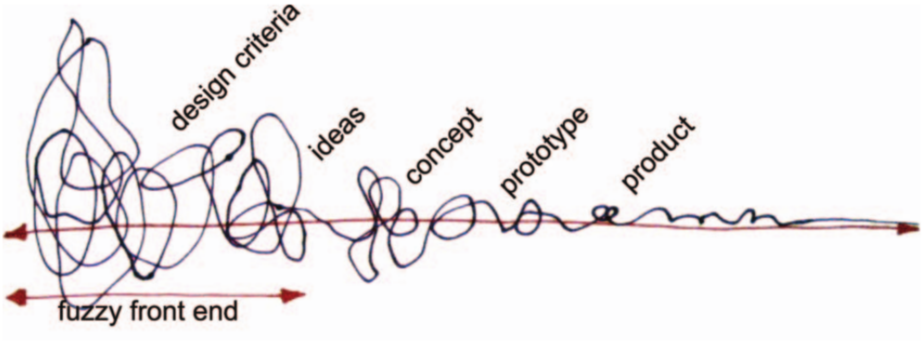


Figure 2.2 PD's more emphasized front end of the design process — a 'fuzzy' front end — and how it ends in a more traditional design process (as depcited by Sanders and Stappers in [66]).

to illustrate how the actions are connected, and to indicate that design process iterations can go both ways [11].

2.2.1 Future Workshop

For the first workshop, Future Workshop (FW) was chosen as a method. In general, to change or transform an actual situation two main approaches can be used: (1) first to criticize the actual situation, then to dream about a preferable future situation, and finally to find ways to move from the actual situation to a preferable one, or; (2) first depict a future preferable situation, then analyze the actual situation, and finally find ways to move from the actual situation to a preferable one [78]. FW belongs to the first approach, and according to Vidal emphasizes: "critique, learning, team work, democracy, and empowerment. This makes FW as a method suitable to support oppressed groups that are struggling for a better living and a better Society" [78, p. 2]. FW was originally developed to engage citizens in Germany and Austria on important issues [38]. In 2005, Vidal wrote:"Now this method is around fifty years old, but the emancipating approach making use of creative working processes and using facilitation methods is by no means out-of date. More recently, FW has been used as a working method of self-controlled learning and a method applicable in the design of new systems, processes and artifacts" [78, p. 3].

A FW usually consists of three phases conducted with a group of participants: *a critique phase* that has the participants list points of critique for their present-day situation; *a fantasy phase* that brainstorms

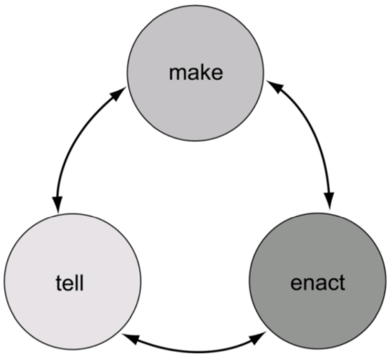


Figure 2.3 The tell-make-enact diagram (as depicted by Brandt et al. in [11]).

utopian visions, and; *an implementation phase* that creates a plan of action for moving towards the utopian visions [11, 78]. All the phases are done collaboratively, but without discussion or objections to any of the critiques or fantasies until the implementation phase [11].

2.2.2 Experience Prototyping

For the second workshop, a prototyping approach called Experience Prototyping was chosen because of the state of the design process at the time. A prototype was (most likely) to be realized by a specific technology, the Leap Motion (see Figure 2.4). Leap Motion is a motion tracking device for Windows and Mac. It tracks in-air hand and finger movement very accurately, almost every little movement, and every big movement. Technically speaking, it creates "8 cubic feet of interactive, three-dimensional space" [43] (see Figure 2.5). The workshop focused on exploring the design possibilities for an authentication system that utilized hand movement by using Experience Prototyping.

As Buchenau and Suri explains: "More and more we find ourselves designing complex and dynamic interactions with converging hardware and software, spaces and services [. . .] This unknown terrain demands new design approaches, specific considerations and, ultimately, the design of integrated and holistic experiences set in context" [13, p. 425]. They suggest Experience Prototyping as a fruitful approach when the subjective experience of interacting with a product, space or system is emphasized [13]. Experience Prototyping is focused on having participants 'experience it themselves'. The basic tenet is that experience is by its nature, subjective, and "the best way to understand the experiential qualities of an interaction is to experience it subjectively" [13, p. 425].

Figure 2.4 Promotional image of the Leap Motion itself (from [43]).

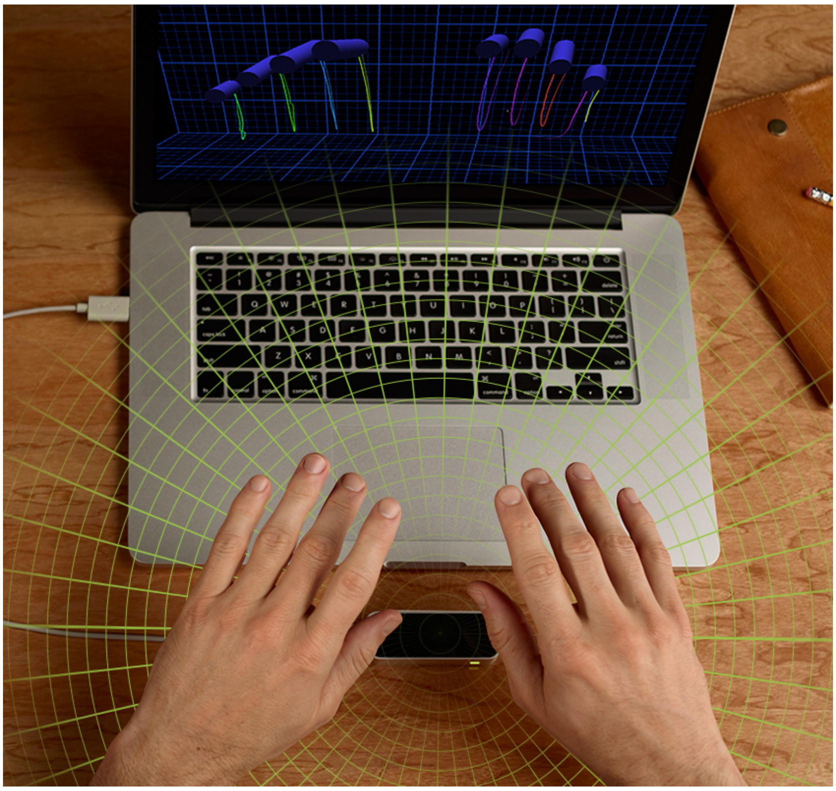


Figure 2.5 Promotional image of the Leap Motion and its interactive, three-dimensional space (from [43]).

In this method, “explorative experiments are carried out by enacting with mock-ups, prototypes or existing products” [11, p. 168]. For participants to express themselves without adopting any abstract formal language, a concept of PD is ‘tacit knowledge’, i.e., personal, experienced knowledge [12]. By having the participants enact with their body limbs, “bodily and perhaps tacit knowledge is set in motion” [11, p. 168]. Enacting refers “to activities where one or more people imagine and act out possible futures by trying things out (by use of the body) in settings that either resemble or are where future activities are likely to take place” [11, p. 164]. According to Brandt et al.: ‘Enacting scenarios by interacting with props or prototypes makes future use situations explicit and hereby subject for enquiry, reflection and learning” [11, p. 168].

2.3 About the Workshops

For this thesis, two design workshops were carried out, both of them had participants as co-designers. The participants in this project are long-term teenage patients that beforehand had agreed to be participants in KULU related research and provided consent. They are patients at Akershus University Hospital (Ahus) in Akershus county of Norway. The participants availability to participate on KULU related research is often restricted by the internal processes the different organizations involved have to follow. During the time frame of this thesis, only two workshops with the participants were possible. Both workshops were executed at the hospital, in Norwegian, with participants that had Norwegian as their mother tongue. Due to other KULU workshops that were to be conducted the same evening, all workshops had to be quite short.

I had the role as facilitator for both the workshops of this project. There were other facilitators for other KULU related research that had their own design stations at the same afternoon and during the same time frame as this project. All the facilitators for all the stations these afternoons changed between the facilitator role of their own station and a helper role, helping out with practical issues for the other stations. This project’s workshops were recorded on audio and the recordings were transcribed. The recording was done with an Iphone in airplane mode — to ensure nothing was accidentally synchronized with Apple’s servers — and transfered to an external hard drive. These recordings have only been stored at this hard drives and the recordings are to be destroyed after the end exam of this thesis at the May 29, 2015. In the transcriptions of the recordings any names of the participants and any information that could expose them were anonymized.

Chapter 3

First Workshop: Future Workshop

This chapter presents the first workshop with the implementation of the method Future Workshop (FW), findings, and discussion of the findings and how it helped me to proceed in the design process and to the next workshop.

The discussion of the findings were based on organizing data, identifying themes, reading, writing, and reviewing design ideas in an iterative process. As Madden explains, to organize and find meaning in qualitative data there are two approaches, usually applied simultaneously: “[1] the idea that data consists of facts that will speak for themselves and [2] that data consists of information that we actively create meaning from as a consequence of our own intellectual and theoretical predispositions” [48, pp. 139-140].

3.1 Why This Method?

FW was chosen as the first methods because of how it suited the research interest of this project. From the use-oriented design cycle (see Figure 2.1), ‘understanding practice’ and ‘identifying needs and wishes’ were the activities for the first workshop. FW is part of a direction where “researchers have sought to enhance and expand the dialogue of participation between designers and users through introducing a change perspective casting a new light on the well known” [11, p. 152]. The critique phase would help to understand how the participants practiced logging in and interacting with authentication, while the fantasy phase would help to identify needs and wishes of authentication. The concept of 'authentication' may be hard to grasp for some, and the critique phase of the workshop also served as an excellent opportunity to make sure that the participants had a certain understanding of the topic and their possible critique related to it. The fantasy phase is the main phase for introducing a change perspective. Fantasizing about utopian ideas would perhaps also serve as a fun and engaging way to identify the needs and wishes of this user group.

Date	November 20, 2014		
Purpose	'Understanding practices and identifying needs and wishes of the topic'		
Topic	'User authentication and login'		
Method	'Future workshop',	25 min total	with 8 participants, age 17–21

Phases		*Time*	*Details*
1	Critique	5 min	Critiquing and discussing the participants' practices within the topic.
2.1	Fantasy	~~12~~ 15 min	Brainstorming utopian, alternate authentication methods.
2.2	Fantasy	~~3~~ 0 min	Discussing which ideas are 'best'.
3	Implementation	5 min	Explaining some of the realistic aspects the utopian ideas will be considered by to narrow down to a design direction.

Table 3.1 Overview of the first workshop with the time changes that happened during execution.

3.2 Implementation

The participants, the location and the time frame of the workshop were decided beforehand by the KULU project. As already mentioned, the participants were teenage patients with long-term illnesses. It was not known how many participants that would be able to participate before the day of the workshop — they are after all patients — but it was a maximum of 12 participants. For this workshop, eight were able to participate. They were between 17 and 21 in age and they all knew each other. The location of the workshop was at the Akershus University Hospital (Ahus). Before the workshop started, the KULU project had planned for pizza with all the participants and facilitators.

Vidal recommends that the room is suitably adapted to the group, creating a cozy, informal, and inspiring atmosphere. Different materials should be available: paper, pin boards, pencils, tape, sticky note blocks, copy machine, transparencies, lab taps, projectors, toys, etc. [78, p. 5]. For this FW, only sticky notes (or 'post it's') and pens were provided, which were to be used for writing critiques and utopian ideas. Vidal also recommends to have the sticky notes on a table or the floor to create a stronger nearness than isolated note writing [78]. The room for the workshop was changed at the day of the workshop, at arrival, and the room became the same room as we ate pizza in before the workshop. Since the time schedule was already quite tight, for practical reasons, the sticky notes were decided to be hung on the wall instead of being stuck to a big paper strip on the table. A big strip of paper was taped to the wall, and the sticky notes were continuously attached to the paper for all the participants to see, as can be seen in Figure 3.1. Because of the quite small size of the room the participants could not get up from behind the table (for those who were seated there) and attach the notes themselves. Therefore I figured that the participants handed me the notes so I could hang them up. The sticky notes for the critique phase had a light red color and those for the fantasy phase had a light green color. This visually showed the amount of critiques and ideas that were stuck to the wall. Those planned for the implementation phase had a light blue color, but ended up not being used.

3.2.1 Topic

Of importance for a FW, is of course the topic or the problem that it will focus on. 'Login and user-authentication' was the topic for all the participants to together, among each other, first, to discuss and criticize, and then, to brainstorm on for alternate solutions. An important aspect was to generate ideas of alternate ways to authenticate or login. 'Login' was part of the topic because of its close relation to user-authentication. It is perhaps close to being synonymous to authentication in everyday language, and I consider it a more accessible, normal term. Since the concept of 'authentication' may be hard to grasp for some, I wanted to use examples as much as possible. Examples likes passwords, PINs, and fingerprints should be good examples to give the participants an understanding of what it is this workshop is about since few people today

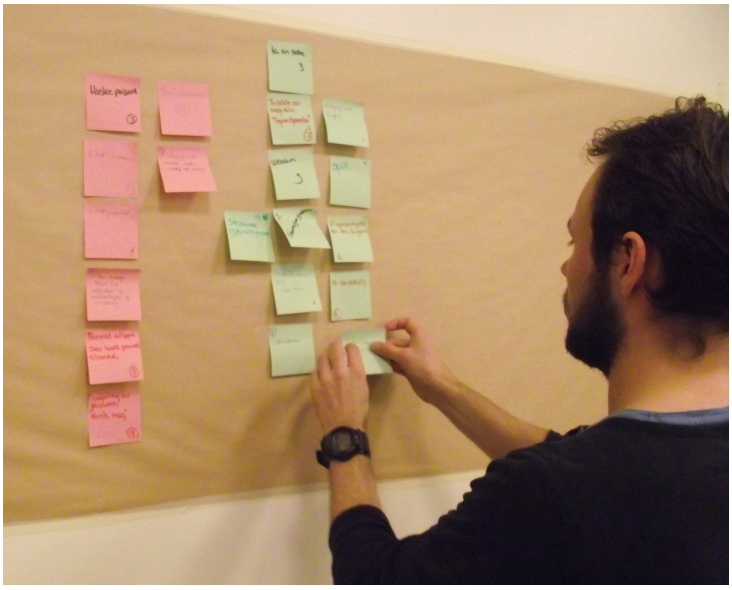


Figure 3.1 Me attaching sticky notes during the fantasy phase.

will ever manage to escape interacting with one of these examples. The more detailed plan for the workshop that was laid out, with subtopics and questions for how to spark the discussion and brainstorming, can be seen in Appendix A.

3.2.2 The Critique Phase

The critique phase was where critiquing and discussion of the topic were to take place. It would help in further understanding the participants practices of authentication. It would also serve as a great way to have the participants together reflect on, become aware of the current situation of login and authentication, and learn about the topic through answering questions, discussing and brainstorming. By critiquing authentication, participants were supposed to implicitly get an understanding of what authentication was and how they used it themselves. Explicitly, the first question was about what different types of authentication or login methods they used. The exact statistics for their usage was not the focus. The focus was to introduce them to the topic of the workshop, and have them realize that they had experience in this area. Secondly, based on the answers the phase would move on to having a discussion about the different authentication methods. Negative critiquing was not explicitly encouraged — in case they mainly were happy with the situation we would talk about that. But as a backup, if the discussion would be still, different questions about the heavy use of passwords today was ready.

3.2.3 The Fantasy Phase

The Fantasy Phase was originally, when Jungk created FW, inspired by research on creativity and innovation, and work on creative problem solving (as cited in [78]). For this phase the well-know brainstorming method is used [78, p. 3]. Utopian, alternate solutions were to be brainstormed. The realistic feasibility of the participants' ideas was not to be criticized by any other in this phase. This is often stated as a rule for the participants during the fantasy phase [11], but for this project it was not mentioned explicitly, but would have been if it was necessary. The wording used to introduced the fantasy phase seemed to be enough for the participant to understand the nature of this phase in that regard:

Me	“We will proceed to the next phase now, which is what we call the fantasy phase, and what we are fantasizing about is a new way of logging in. It does not need to be bound in realism at all. It can be crazy, strange, funny, illogical ideas. [. . .]”
Girl 3 (age 17)	“What did you say we are writing about now?”
Girl 4 (age 18)	“How you can log in different places.”
Me	“Yes. So a new way to log in, something that can replace passwords. [. . .] For instance, what is the simplest, or what is the most fun way to log in.”

What was actually said during the workshop deviates from the plan of what to say, which is included in Appendix A. This is only natural though, as the path of a natural discussion always will have an element of openness. The plan of what to say did mostly serve as a backup plan in case I got stuck or forgot what to say.

In the normal second step of the fantasy phase, it is recommended that “the most promising ideas have to be transformed, that is, they must be reduced to a possible and realizable core. Ideas have to be prioritized after a common analysis and evaluation” [78, pp. 7-8]. From the workshop schedule, this step did not have much time — approximately 3 minutes — but it was not a grandiose plan either. The participants would simply say which ideas they liked the most, possibly helping in narrowing down the next step in the design process. This step was not executed as planned because of what may be a lack togetherness. As Vidal writes: “In the classical FW all participants write down the points on a big sheet of paper lying on the ground or on a table. Later, the points are cut out and grouped. This method creates a stronger nearness than isolated note writing” [78, p. 6]. At this point in the workshop the participants had started discussing and brainstorming together in smaller groupings, and getting them to work on one task all together did not happen. I tried to engage them in choosing the best ideas; some partook, but so few that I did not consider these results as findings. This was not necessarily negative. The topic was, admittedly a bit of surprise for me, something they found interesting enough to discuss further on their own initiative. All of these discussions were not dead serious, but, in a teen spirit, filled with humor about their ideas and possible scenarios of use.

3.2.4 The Implementation Phase

The implementation phase was the phase sat off the least amount of time for. The realistic aspects of the ideas were mostly to be discussed after the workshop, based on relevant literature. Though sticky notes had been prepared for this phase, again, it was planned that the participants would mostly get an explanation about the realistic aspects that the utopian ideas would have to be considered by, i.e., being able to perform as authentication, some security aspects, the state of related technology, and most of all design concepts for a design that satisfied them.

3.3 Findings

Eight participants were able to participate in the first workshop. They were teenage, long-term patients at the age between 17 and 21. They were all participating in the future workshop at the same time, discussing and brainstorming together. All of them knew each other and several of them seemed to be very good friends, which may have contributed to the good atmosphere for participation that emerged. Almost all of them were engaged and they did not seem to be shy, or afraid of mentioning challenges they may have because of their health challenges.

3.3.1 The Critique Phase: Teenagers and Login Habits

The critique phase of the future workshop was intended to both learn about the participants' experiences with logging in and authentication in general, but also to serve as a learning process for the participants — by 'telling' and imagining from questioning, discussing, and brainstorming. By critiquing authentication and logging in, participants were supposed to implicitly get an understanding of what authentication was and how they used it themselves. Explicitly, the first question was about what different types of authentication or login methods they used. As examples to start them off were password and Facebook's login solution, and that stirred a conversation right away. Facebook's login solution is a solution websites can integrate into their sites — enabling users to sign up and login using their Facebook accounts. The first participant to engage said he almost always used Facebook login, and another stated he used it whenever possible. Several of the participants used ID tokens for their Internet bank. At least one participant used fingerprint to unlock her phone, and everyone had used passwords and PINs. The exact statistics for their usage were not the focus, and very likely many of them used all of these ways of authentication. The focus was to introduce them to the topic of the workshop, and have them understand that they had experience in this area.

Too Many Passwords

Next we moved on to critiquing passwords. Their struggles with passwords were particularly the amount of and requirements for passwords. The first critique was on the amount of passwords:

> "I think that it is too much, or too many things, that you have password for. So for me it can sometimes be hard to remember the password I have for each login, because it's not always I can use the same password. So for me it gets like I really have to [. . .] think about what password I have for the different sites." (Girl, age 17)

Another stated that she tried to use the same password as far as possible, even though she thought she knew it was more ‘hackable’. And one was annoyed with password requirements of length and numbers, and the differences between sites:

> “Personally I hate when the service says that your password isn’t good enough [he starts mimicking the services]: ‘you need two numbers’, ‘you need at least that many capital letters’, or something. [. . .] I would rather have three passwords that I use, but sometimes I have 19 different ones [. . .] As a result, I have eight different variations I try every time I’m logging in.” (Boy, age 17)

A female participant also disliked when her passwords expired, forcing her to change passwords. She also said that she would often share her password with others so they could log in as her when she was too tired.

Security and Privacy

As mentioned, some participants used Facebook’s login service when logging in or signing up for sites. When asked about if they had any critiques on this service, privacy and security came up. Regarding privacy, a participant did not trust Facebook; mentioning that he was afraid of what information the site he logged into could acquire, or that something could suddenly be posted to his ‘Facebook wall’. Another participant was concerned about when cookies stored her username and password, e.g., when she had checked off on a ‘remember me’ box when logging in, and that someone could easily get access to her accounts if accessing her computer. In that regard, a participant felt that logging in through a social media’s single login solution was not very secure, since several user accounts then would be dependent on the security of a single site and password, but the convenience and speed of using such solutions often made him choose that.

3.3.2 Fantasy Phase: Alternative Authentication

When I gave the participants hints on fantasizing about an authentication method, I mentioned that it could be something ‘crazy’, ‘strange’, ‘funny’, ‘illogical’, or ‘simple’. The suggested ideas, as can be seen in Table 3.2 (or matrix), did broadly reflect all the given hints. I did not ask them right away for new ideas of authenticating, as I did not want them to feel any pressure that could choke the brainstorming before it had begun. I asked if they could think of other ways to authenticate. Also, not explicitly asking for new ways of authentication could possibly stronger flourish co-realization and learning. Learning was important through out the whole process because of the, perhaps, abstract subject of authentication.

In the beginning of the fantasy phase there was some confusion of what we were going to do: "are we going to think about new ways of login?" I tried to clarify with saying that we were going to think about something that could replace passwords. Not explicitly saying 'new', but it unintentionally implied 'new' — which was a good thing, since I wanted 'new'. I did not have to explicitly say 'new', the brainstorming within the group brought it there. The participants had an impressive knowledge and understanding of existing and possible alternative ways of authentication. There was never a need to explain the difference between the user credential, authentication, and identification. Though it did get mixed up a few times, I was afraid that explaining this in detail would be off putting for their engagement.

Since the ideas of the participants focused on replacing passwords, and since a password is a user credential in authentication; the ideas were mostly user credentials that could serve as authentication factors. In many of the ideas there seemed to be a trait of low intrusion on user interaction. Low intrusion is often said about *biometrics* in computer security literature. Many of the ideas fell under the 'biometric' category. Biometrics are used as authentication by using a biometric that is distinguishable enough to be used for user authentication [56]. Biometrics are usually classified within physiological or behavioral biometrics. "The physical type includes biometrics based on stable body features, such as fingerprint, face, iris, and hand" [56, p. 2025]. Behavioral biometrics "relates to the specific behavior of a human (user) along time in performing some task" [53, p. 156]. Tasks such as movement, gait, gestures, keystroke dynamics (typing), signature writing and voice. For the participants to have low intruding ideas for authentication may only be natural since security often is considered 'in the way' [55, 67]. This aspect of authentication can be related to *usability*, but also *accessibility* from a conceptual perspective. Accessibility was further related from a physical perspective to the idea 'dance':

Alternative authentication ideas (in alphabetical order, left to right)

BMI (Body Mass Index)	Movement	Dance	Tell a dirty joke
One time pass code via phone. Works with all websites.	A particular expression in picture	Fingerprints of all your fingers	ID tag(s)
High pitched sound (for teenagers)	Hair login; DNA recognition	Login using your tongue	IP address
Iris/Eye scan	Odor	Breath	Site a line from a religious text or movie.
Scanning of scars	Scan entire body	Game	Voice recognition
Voice recognition	Sweat	Take a picture of myself; recognized.	Take a selfie
Drawing	Very personal quiz	Web-cam	Ear recognition

Table 3.2 A matrix of all the ideas for alternative authentication methods from the fantasy phase.

Me “What about dance for example? It can also be-”

Participant “It can be a bit difficult for some.”

“[. . .]”

Participant “Wheelchair dance.”

Me “You can dance with your arms.”

There were also other aspects that were harder to categorize. Several ideas from the brainstorming seemed to be more than only ‘usability’ related, they were appealing to the participants in other ways. Some ideas were clearly connected to popular media, perhaps especially the science fiction genre (sci-fi). Novel forms of technology is often envisioned in sci-fi books, movies and games first. ‘Iris scanning’ was suggested early in the brainstorming as something a participant knew was a method for authentication: “And you have the classic one from James Bond, with iris scanning.” (Boy, age 19)

Other ideas they found enjoyable in other ways — laughing of some ideas, and saying “I have a cool idea” and “think how fun”. ‘Fun’ is a descriptive term in itself, but ‘cool’ is harder to know what means. From the context, the participants used the term to express how they felt about the ideas they fantasized of — how positively interesting and enjoyable it would have been to see them in action. I have chosen to relate these additional focuses of the participants to *User Experience* (UX). Loosely, Table 3.3 shows how I related the ideas to these different design aspects. Usability, accessibility and UX will be discussed in the next section.

‘Low intrusion’:	face and voice related ideas, other biometric ideas, and ID tag
‘Cool’:	voice related ideas, taking a selfie, game, dance, drawing, and iris scanning
‘Fun’:	dance, movement, drawing, game, voice, telling a dirty joke, and logging in with your tongue

Table 3.3 My interpretation of the participants’ relations to their ideas.

3.4 Discussion: Usability, Accessibility, and UX

From the ideas of the participants I found traits of low intrusion on human interaction. ‘Non-intrusive’ is a term often used about facial recognition in computer security (e.g., [33]). What non-intrusive means in form of design concepts are not specified, but from the context, since biometrics have the potential to simply scan the user to log him/her in, ‘non-intrusion’ refers to the potential for no interaction for the person in the process of authentication. As how I see UX to relate to the participant’s ideas, I feel it is important to once more point out that the participants were teenagers (or young adults), in the ages between 17 to 21. So some of these ideas were not only appealing, but had teenage appeal.

3.4.1 Usable and Accessible Authentication

When aiming for good usability in a design it is according to Benyon normally focused on: *efficiency* — that people will be able to do things using an appropriate amount of effort; *effectiveness* — that the design contains the appropriate functions and information, appropriately organized; *easy* to learn how to do things and recognize/recall how to do them; *safe* to operate, and; *high utility* in that it does the things that users wants to get done [7]. The different focuses of usability are applied as necessary in relation to the design context, and an authentication method is special in how usability could normally apply. Authentication is just a step on the way of the user's intension. Low intrusion in authentication makes sense for the overall usability of an application — that the authentication does not intrude in a user's use of an application. Low intrusion also makes sense from how often a person may authenticate when using the Web. For password and PIN based authentication, the form of the authentication factor is often mainly what makes them intrusive. For example, a password must be created from requirements, remembered and changed by the user, time and time again. This is the core issue of this authentication method. Not in, e.g., how the web-form for the login procedure is designed. Compared to the issues of the password itself and the related security practices — the web forms are trivial. From Benyon's list of the focuses of usability, low intrusion would be within 'efficiency' — not requiring a large amount of effort, and 'high utility' — in that it does the things that people want to get done. The possible accessibility issue of passwords is also connected with the memory load — a conceptual accessibility issue, which is solved by focusing on these usability aspects.

The first step in the design process must be to decide the user credential(s) and the authentication factor(s) of the authentication method. The surrounding design and infrastructural context of an authentication method (e.g., a web-form and a website) is there to support the use and understanding of the user credential(s). It can be argued that a too invisible authentication method could be a privacy intrusive. A degree of transparency should be maintained — the user should know that s/he is in the process of being authenticated. This should be the job of the surrounding context the user credential(s) is within. This contexts is where the remaining usual ingredients of usability would apply: 'effective', 'easy to learn', and 'safe'.

3.4.2 Cool and Fun UX

The International Standards Organisation (ISO) defines usability as: "[...] the effectiveness, efficiency, and satisfaction with which specified users can achieve specified goals in particular environments" (as cited in [34]). *Satisfaction* in this definition refers to the comfort and acceptability of product use. Acceptability within usability is further said to be political, convenience, cultural and social habits, usefulness, and economic [7]. Several of the ideas from the participants were appealing to them, and/or they were engagingly presented and discussed during the workshop. This project follows the premise that these ideas share common elements that interests this user group, and that this may be an aspect of a future design they will find satisfactory.

The satisfaction component of usability has been concerned about avoiding negative feelings, e.g., tiredness, discomfort, frustration and personal effort, rather than producing overtly positive emotions [28, 34]. As Jordan says, it is possible that making a product usable — usability wise — will guarantee a satisfactory design, but if it does not, the design will fall short [34]. 'Cool' and 'fun' were descriptively used by the participants during the workshop, and I will use them as pointers for design concepts to use in the further discussion of the design decisions for the next workshop.

Figure 3.2 shows how Hassenzahl and Tractinsky views UX today to have a total of three parent perspectives: 'going beyond the instrumental', 'emotion and affect' and 'the experiential' [28]. HCI's early days, with an instrumental focus on the task of a technology, were among other challenged by the importance of beauty, i.e., aesthetics [28]. Later, it has been argued for the importance of surprise, diversion, intimacy, stimulation, identification, and evocation in HCI design [28]. All of these approaches have a common goal: "to enrich current models of product quality with non-instrumental aspects to create a more complete, holistic HCI" [28, p. 93]. When UX started to emerge, there were discussions if it could be considered part of HCI. For simplicity, this thesis will consider it part of HCI today.

The *emotion and effect* perspective focuses on positive emotional outcomes such as joy, fun and pride [28]. There are two basic ways of dealing with emotion in UX: one way stresses the emotional consequences of use, the other, the preceding emotions of product use and evaluative judgments [28]. The *experiential* "perspective on UX emphasizes two aspects of technology use: its situatedness and its temporality. In this view, an experience is a unique combination of various elements,

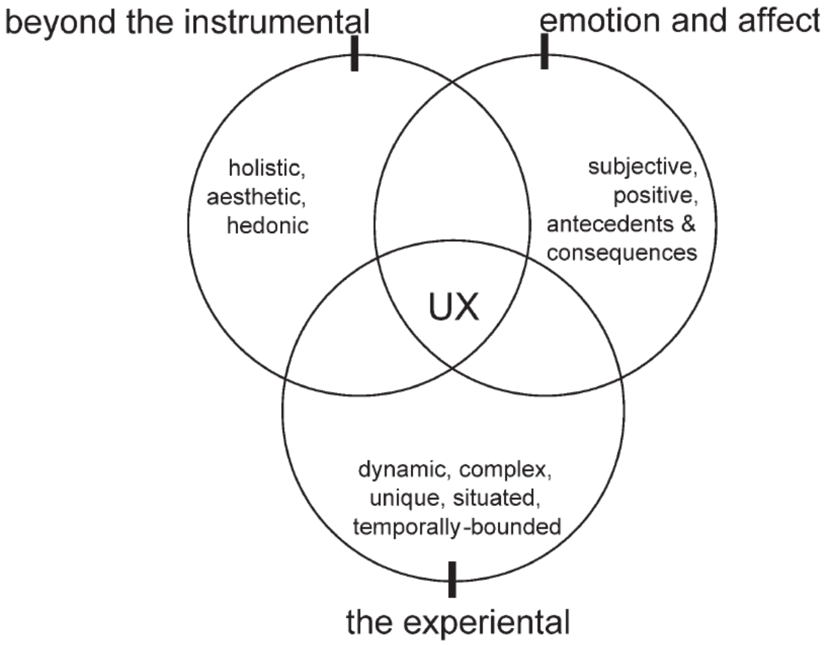

beyond the instrumental
emotion and affect
holistic, aesthetic, hedonic
subjective, positive, antecedents & consequences
UX
dynamic, complex, unique, situated, temporally-bounded
the experiental

Figure 3.2 Hassenzahl and Tractinsky's depiction of what defines UX today [28].

such as the product and internal states of the user (e.g. mood, expectations, active goals), which extends over time with a definitive beginning and end" [28, p. 94]. McCarthy and Wright highlights the need to take a holistic approach to UX (as cited in [7]). Their argument is that "experiences have to be understood as a whole and cannot be broken down into their constituent parts, because experience lies in the relations between the parts" (as cited in [7, p. 99]). Benyon builds on McCarthy and Wright, and concludes: "McCarthy and Wright take a stance that emphasizes the rights of people to have the experiences they need and desire rather than having experiences thrust upon them by poor designs. [. . .] Experiences, therefore, cannot really be designed. Designers can design *for* experience, but it is individuals and groups who have the experience" [7, p. 99].

Cool Design

Culén and Gasparini explain the intricate grammatical meaning of the word cool as the following:

> "It is ironic and rather interesting that the word 'cool' may be used as a synonym for two classes of adjectives, a verb

> or a noun. In the first adjective class it can mean: cold, chilly, annoyed, apathetic, frigid, impertinent, indifferent, insolent, lukewarm, offish, precocious, reserved, standoffish, unapproachable, uncommunicative, unenthusiastic, or unwelcoming. In the second adjective class it can mean: beautiful, divine, exquisite, fashionable, fun, glorious, hip, hunky-dory, trendy, neat, nifty, peachy, popular, sensational, stylish, subzero, swell, well designed. As a verb it can mean: calm, calm down, chill, compose, control, dampen, lessen, moderate, quiet, reduce, rein, repress, restrain, simmer down, suppress, temper as well as go with the flow, hang easy, lay back, let go, let it all hang out, let up, mellow out, moderate, quell, recede, reduce, slacken, slow, subdue, subside, take it easy. Finally, as a noun it can mean: assuredness, bliss, common sense, dude, king, endurance, poise. Out of context, the word 'cool' has paradoxical tendencies." [19, pp. 117-118]

Teenagers connection with 'cool' has according to Frank, and later Moore, "been associated with behaviours around authenticity and laid backed-ness and is rooted in an urge to challenge convention" (as cited in [32, p. 76]). Neumeister explains that since the 1960s it has been detached from adult culture and has become associated with an 'I want that!' attitude" (as cited in [32]). For Southgate 'the cool' are always looking to be different so that they can express themselves in an authentic manner (as cited in [32]). Sundar et al. views cool as socially constructed, but a possible and positive attribute of a product, and stresses that cool is an evolving idea which is in a state of constant change causing the perception of cool to be temporarily unstable (as cited in [47]).

Based on a suite of studies with children and teenagers, Read et al. have added more concretely in the form of eight design guidelines to the understanding of 'cool' [62]:

1. *Cool is expensive* — cool design does not look cheap, gives the user value derived from achievement, and is rare.

2. *Cool is real* — cool design utilizes authentic technology and trends, and it is innovative.

3. *Cool is retro* — cool design gives the user associations to familiar or global retro.

4. *Cool is both social and antisocial* — cool design gives the user options of whom to communicate with, which may give users the feeling of being part of an exclusive group.

5. *Cool is innovative* — cool design is innovative in that it appropriates technologies in novel and unusual ways and unusual situations.

6. *Cool is rebellious* — cool design incorporate some rebellious appearance or feature, the support for personalization, and the possibility for breaking the rules.

7. *Cool is attractive* — cool design is attractive and does not make the user look unattractive.

8. *Cool is inherent* — cool design does not emphasize sides of the teenage users' life they can not control.

Read et al. explains 'cool' as "more than a design ideal", they have a belief that rather than being providing a formula for cool, their design guidelines are better applied in a reverse way in order to design products that are at least not entirely uncool [62, p. 9]. "We propose that interaction designers can dip into our design ideas and apply one or more of these principles to create better products" [62, p. 9]. In relation to UX, the guidelines of Read et al. are very focused on aesthetics and preceding emotions related to use, but also some on the emotional consequences of use when it comes to personalization and not emphasizing sides of the teenagers' life they can not control.

Fun

Wikipedia gives a general explanation of 'fun' as the following: "Fun is the enjoyment of pleasure" [25]. When fun is the enjoyment of pleasure, to design 'fun', designers must first design for pleasure. Patrick Jordan argues that designing for pleasure can be as important as usability (as cited in [7]). Jordan describes pleasure as being "the condition of consciousness or sensation induced by the enjoyment or anticipation of what is felt or viewed as good or desirable; enjoyment, delight, gratification" (as quoted in [7]).

"A distinction between enjoyment and fun is difficult but possible to articulate, fun being a more spontaneous, playful, or active event" [25]. With this distinction, designers must design something that is pleasurable in a distinct way, by being a spontaneous, playful, and/or active event. Kare Holtzblatt defines joy as human beings' autonomic response to our encounter with the world. Her definition of joy has close relations to fun in its spontaneousness. "Joy is pulled unknowingly and unwillingly from within" [31, p. 40]. For Holtzblatt, joy contributes to the understanding of why the experience of cool is so compelling [31]. She presents joy as the absolute center of cool. Joy does not come from a specific feature, or aesthetics, but emerges when products satisfy a number of key motivations: accomplishment, connection, identity, and sensation [31]. The *accomplishment* a person experiences when an artifact empowers the person to fulfill the many intents in life. The *connection* that is enabled for a person to make relationships that matter more real and manageable. *Identity* seeking functionality that helps people find ideas of who they may be. The *sensation* that can be had from both sensory immersion and moments of pure sensual delight.

Lionel Tiger has developed a framework of four dimensions for understanding pleasure: *physio-pleasure* is the pleasures related to sensing — seeing, hearing, touching, handling and smelling; *socio-pleasure* arises from relationships with others, e.g., the pleasure from using social media; *psycho-pleasure* refers to cognitive or emotional pleasure, e.g., the perceived ease of use and effectiveness of a device, and the satisfaction of acquiring new skills, and; *ideo-pleasure* "concerns people's values — things one holds dear or meaningful — and aspirations" (as cited in [7, p. 103]).

Designers within 'fun' mentions that it rarely should come before usability in an end product, as frustration for a user from lack of usability can suppress a 'user experience', but it can co-exist [21, 71].

3.5 Related Research: Authentication and UX

Forlizzi and Battarbee says UX has been associated with a wide variety of meanings (as cited in [28]), "ranging from traditional usability to beauty, hedonic, affective or experiential aspects of technology use" [28, p. 91]. Several studies in the design of authentication have focused on creating a good user experience by (only) looking at the usability and/or perceived security of a design (e.g., [10, 41, 45]). When understanding UX as more than a good user experience from usability, i.e., going beyond the instrumental, there are not much research on authentication and

UX.

In 2011, Cohen et al. conducted an experiment for understanding adoption of new technology by testing the satisfaction of using a fingerprint based authentication with a group of younger people, and a group of older: “The results showed that the probability of successful authentication had a significant main effect on the perceived reliability and user satisfaction” [18, p. 449].

Perhaps the most relevant study is by Karlesky et al., published in 2013, who explored a behavioral biometric authentication using Microsoft Kinect to capture gestures from the entire body to unlock doorways [37]. They aimed to give pleasure in use inspired by research that links bodily movement/posture to human emotional state. The data from user tests was interpreted to show promise of a pleasurable and playful design.

Budde et al. published a study in 2014, where 22 participants of ages between 20 to 40 tried six different ways of authentication when connecting to a Wi-Fi hotspot from a phone [14]. This meant that the different ways of authentication were confirming that the user was in a specific context where s/he should be allowed to use the Wi-Fi network, e.g., a hotel lobby. The participants evaluated the ways of authentication using two standardized questionnaires — the Systems Usability Scale (SUS) and User Experience Questionnaire (UEQ) — and qualitative statements from some participants were collected [14]. The ways of authentication were ‘username:password’, ‘QR code’, ‘Near Field Communication (NFC)’, ‘Two-Dimensional Signal Transmission (2DST) waveguide sheet’ (a sheet a phone can be laid on to confirm that the person is at an approved location), ‘Microsoft Kinect’, and ‘Audio context’. The research had a different context for the authenticating method than this project, so, aside from ‘username:password’, only Kinect and NFC can be considered relevant and general applicable ways of authentication. NFC was the only method that all participants understood the first time they used it. It had no apparent usability issues and was considered attractive by the ratings from the questionnaires. The participants commented on it as intuitive and fast. When using the Kinect some participants had to repeat their authentication attempt(s). On the Kinect the participants commented that it was fast, intuitive and cool, but some were embarrassed and some felt it was a privacy intrusive — that they were under surveillance (this could perhaps be related to ‘surveillance’ being the recurrent topic of critique when Microsoft, in 2013, launched the Xbox One that featured the Kinect 2.0 [30, 36, 75, 83]). Budde et al. concluded that the context of use must be considered when using visible activity to authenticate — will the user be embarrassed when authenticating? Otherwise, authentication with NFC and Kinect were the two methods that required the least amount of time for the users to authenticate.

In 2014, Aumi and Kratz published a study involving a behavioral biometric authentication technology called the Air Auth [4]. The Air Auth uses in-air hand gestures as a user credential. It tracks biometric data by using a short range depth sensor. The data enables the decoding of a user's secret hand gesture, classifying the biometric properties of the user's hand, and classifying the movement style of the user. They conducted four user-studies to find: (1) suitable hand movements for authentication, (2) the accuracy of the technology, (3) the resilience towards security threats, and (4) similarity and repeatability of the gestures over time in a longitudinal study. In the second user-study the participants' feelings and experience from performing the gestures were rated using the Emo Card technique to see how user-ratings on easiness, pleasantness and excitement of a gesture correlates to accuracy. High pleasantness and excitement did have a significant effect on the accuracy when performing the gestures. Aumi and Kratz collected some comments about why particular participants would prefer the Air Auth as authentication: "'simple and faster', 'more secure than traditional approaches', 'simply cool'. One participant commented: 'It's great because I do not have to touch my phone when I am cooking. I would like to use similar techniques to do more stuff like receiving calls and reading text messages'" [4, p. 315]. Some participants felt it would be awkward to do the gestures in public.

Not many studies within user-authentication and HCI goes beyond the instrumental. Computer security have been said to lack a focus on usability [35], and it seems like the design of authentication also lacks a focus on UX.

3.6 Discussion: Authentication Factors

When conducting the future workshop, the usual implementation phase had to be minimal (5 minutes) because of the scheduled time frame planned by the KULU project. The realistic aspects of the participants' suggested authentication methods would quite possibly have required more time than the time scheduled for the entire future workshop. Some ideas of the participants were not usable as authentication. This discussion of the future workshop does in a way continue the implementation phase by reviewing relevant design and security literature to narrow down the choices of a final design. Even though security is not the point of view for this project, an authentication has to be able to perform as just that — an authentication. This necessarily involves some aspects of security on the human interaction side. The following literature review in this chapter also aims to fill that void. The infrastructural boundaries of the Web are not taken into account for this step of the design process (or any of the steps documented in this thesis).

This part of the discussion starts with what, according to Vidal, is the usual second step of the fantasy phase where it is recommended that "the most promising ideas have to be transformed, that is, they must be reduced to a possible and realizable core. Ideas have to be prioritized after a common analysis and evaluation" [78, pp. 7-8]. Thus the steps of this part of the discussion are:

- Reviewing the ideas so the most promising ideas are reduced to a possible and realizable core.
- Continue the implementation phase by reviewing relevant design and security literature to find the next step on the path towards a final design.

3.6.1 To the Realizable Core

Some suggestions for alternatives to passwords may only have had the traits crazy, strange or illogical, e.g., 'by telling a dirty joke', logging in 'with your tongue', or 'by scanning your scars'. The two latter being rather unpractical. Other suggestions would also be unpractical in a login procedure. Like authentication by 'dance', 'DNA from your hair', or 'ear print'. Three suggestions could not be considered applicable as ways to authenticate individuals: 'IP address', 'detection of a high pitched sound', and 'BMI' (body mass index). An IP address can be used as an identity, but is never reliable as authentication. IP addresses are, however, location based, and location based authentication is an authentication concept [5]. So in relation to the IP-address suggestion, I did mention that it was location based to see if this was something any would like to take further as an idea, but it was not further explored during the workshop. This was perhaps too much to expect, even if they were 'tech savvy' teenagers. The detection of a high pitched sound can perhaps identify groups of people, e.g., teenagers — which was the idea — but not authenticate individuals. BMI is not unique enough to serve as authentication.

'Sweat', 'odor', and 'breath' may be highly accurate authentication methods sometime in the future. Authentication by breath, for instance, may be realized by a proposed technology that apparently authenticates by breath waveform [57]. These ideas, however, was decided to be too futuristic for this project.

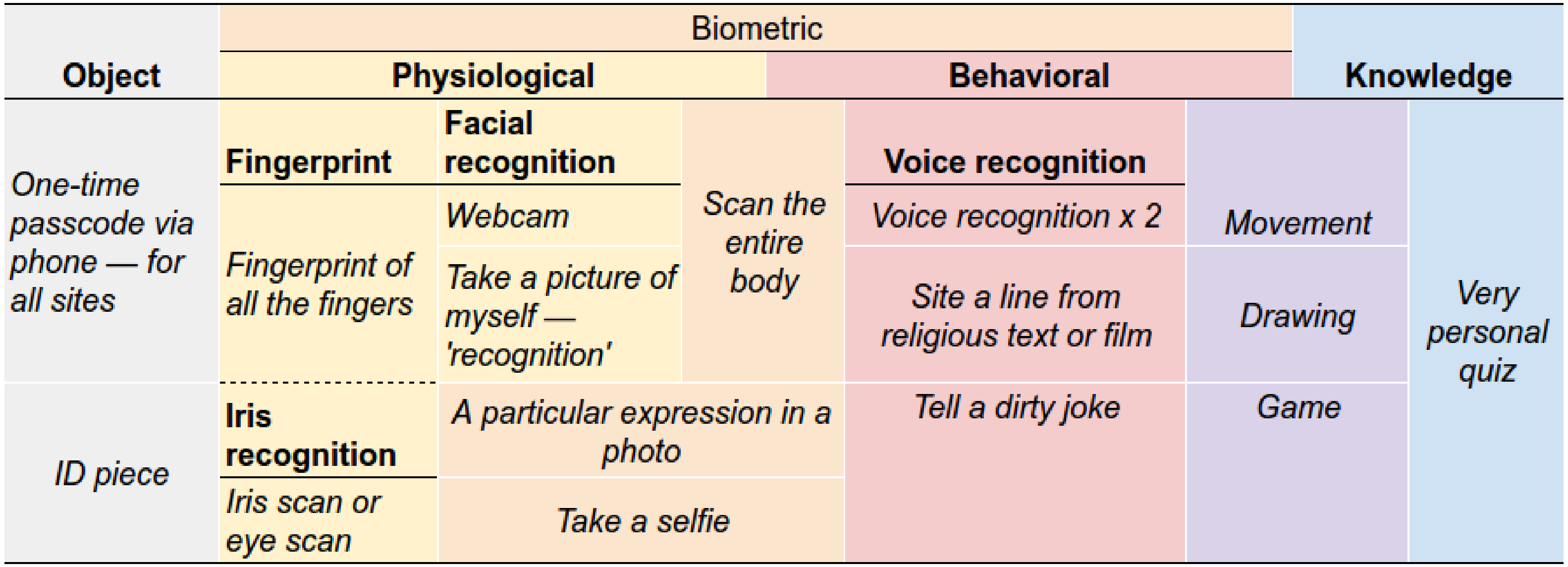
Figure 3.3 lists the groups of remaining ideas categorized after the relevant user authentication categories: object based authentication, physiological and behavioral biometrics, and knowledge based authentication. Several ideas has the potential for two authentication factors. The base categories for the authentication factor are 'what you have', 'what you know', or 'what you are' [46, 49, 56, 72]. "[D]ifferent types of authenticating factors can be combined — creating a multi-factor authentication process [56].

3.6.2 Object and Knowledge vs. Biometrics

Object based authentication is classically a door key, or more 'digitally' — an access or smart card. The authenticating element is that it is an object the rightful user has. *Knowledge based* authentication authenticate on the premise that it is a secret only the user knows, e.g., password, PIN, or quizzes.

Biometric systems offer several advantages over traditional authentication schemes. According to Jain et al.: "They are inherently more reliable than password-based authentication as biometric traits cannot be lost or forgotten (passwords can be lost or forgotten); biometric traits are difficult to copy, share, and distribute (passwords can be announced in hacker websites); and they require the person being authenticated to be present at the time and point of authentication (conniving users can deny that they have shared the password). It is difficult to forge biometrics (it requires more time, money, experience, access privileges) and it is unlikely for a user to repudiate having accessed the digital content using biometrics. Thus, a biometrics-based authentication scheme is a powerful alternative to traditional authentication schemes" [33, p. 125].

The dominant knowledge/object based authentication methods have to add another complication for the user in able to more certainly authenticate, e.g., password and a one time code via SMS. Here, two different knowledge based mechanisms are used, and the last one also incorporating an object (the phone). Biometrics are potentially less intrusive in this regard. As they are potentially unique, some biometrics are such strong authentication factors in themselves that the need to combine them with additional factors is lower.



<table>
<tr><th rowspan="3">Object</th><th colspan="5">Biometric</th><th rowspan="3">Knowledge</th></tr>
<tr><th colspan="3">Physiological</th><th colspan="2">Behavioral</th></tr>
<tr><th></th><th></th><th></th><th></th><th></th></tr>
<tr><td rowspan="3">One-time passcode via phone — for all sites</td><td>Fingerprint</td><td>Facial recognition</td><td rowspan="3">Scan the entire body</td><td>Voice recognition</td><td rowspan="2">Movement</td><td rowspan="5">Very personal quiz</td></tr>
<tr><td rowspan="2">Fingerprint of all the fingers</td><td>Webcam</td><td>Voice recognition x 2</td></tr>
<tr><td>Take a picture of myself — 'recognition'</td><td>Site a line from religious text or film</td><td>Drawing</td></tr>
<tr><td rowspan="2">ID piece</td><td>Iris recognition</td><td colspan="2">A particular expression in a photo</td><td rowspan="2">Tell a dirty joke</td><td rowspan="2">Game</td></tr>
<tr><td>Iris scan or eye scan</td><td colspan="2">Take a selfie</td></tr>
</table>

Figure 3.3 Alternative authentication ideas grouped by categories of authentication factors. I have related some ideas to more than one category and/or subcategory.

The idea 'one-time pass-code to the phone' may be practical in the sense that many always carry their phone. This ideas made its way into the next workshop for evaluation, as part of a questionnaire. Of the other ideas that purely belongs to the object and knowledge based authentication, I decided to not progress with 'ID token' and 'very personal quiz'. A 'very personal quiz', even though it is probably easier to remember than a password, could still be a heavy memory load — perhaps several questions, and it could take a while to complete. Personal information is in general potentially weak against *social engineering* attacks [9]. Social engineering techniques involve an attacker tricking the user into believing that s/he (the user) needs to provide specific information or perform a specific action [72]. The leaking of a users answers can be critical in two ways; access to hers/his accounts, and the leaking of personal secrets from the quiz. An ID token may be an easy way to authenticate him/her self with, but it can be lost or stolen. At first I thought that it may not be 'cool', but if the token is the user's phone or in the form of a bracelet, then perhaps. I did, however, instead decide to bring along the 'one-time pass-code to the phone' idea to the next workshop. ID token may have been suggested based on something the participant already knew was an authentication method, and not necessarily a wish — since ID token was mentioned in the critique phase as a method used by banks.

3.6.3 Physiological Biometrics

As how the dominant authentications work, when they meet the human user it behaves as an obstacle for the user's intention — these schemes are quite intrusive. Sasse and Flechais claims that "[e]ven a very usable security mechanism is likely to create extra work from the users' point of view. It is human nature to look for shortcuts [. . .]" [67, p. 15]. Biometrics have the potential to be very 'usable' in terms of low intrusion.

'Iris scanning' was suggested early in the brainstorming as something a participant knew was a way of authentication: "the classic one from James Bond, with iris scanning" (male participant). The iris is considered to be a very unique and stable biometric [33], but the current use of iris scanning is mainly at government agencies and major companies [17]. According to Clover Apple bought a company that specializes in iris and other biometrics related technology, but it is not a technology that is mainstream or easy to acquire yet [17]. It may also be viewed as a creepy way of authentication because of how a unique biometric it is. Popular media has presented it as privacy invading technology [59]. Because of this 'seriousness' of this authentication, I decided to not bring iris scanning along for the next workshop, but it did come up in discussion during the second workshop.

One suggestion was 'fingerprints of all fingers'. Fingerprint authentication technology was introduced in the major commercial product, the Iphone 5S. Because of the high number of false negatives of the fingerprint technology, and since the security is still dependent on a PIN/password fallback, it is currently mainly considered a practicality compared to the usual PIN or password [39]. "Multiple fingerprints of a person provide additional information to allow for large-scale identification involving millions of identities. One problem with the current fingerprint recognition systems is that they require a large amount of computational resources, especially when operating in the identification mode. Finally, fingerprints of a small fraction of the population may be unsuitable for the automatic identification because of genetic factors, aging, environmental, or occupational reasons (e.g., manual workers may have a large number of cuts and bruises on their fingerprints that keep changing)" [33, p. 126]. Because of the low intrusion rate and that it is on the Iphone I decided to bring fingerprint along to the second workshop in form of discussion and on a survey for the participants to rate.

Four suggestions were related to face recognition. When I gave hints to what the ideas in the fantasy phase could be, I mentioned 'simple' (among crazy, strange, funny, illogical). This may have triggered some participants to think about the most convenient way, or least intrusive way, of authenticating, which is something that can be said about facial recognition. Staring at a device to obtain information is usually an initial step of interaction. What if we were instantly authenticated just by putting our face in front of the device. The idea that a digital entity recognizes a person — just as a person recognizes a person — can naturally seem only natural to a person.

"Face recognition is a nonintrusive method, and facial images are probably the most common biometric characteristic used by humans to make personal recognition. The applications of facial recognition range from a static, controlled 'mugshot' authentication to a dynamic, uncontrolled face identification in a cluttered background" [33, p. 126]. Face recognition systems (FRSs) have had a range of algorithmically barriers to overcome like: often requiring a fixed and simple background or special illumination, and the difficulty in matching images captured from two drastically different views and under different illumination conditions [33]. Still, since four ideas were related to facial recognition, I decided to bring it along in the survey for the second workshop.

3.6.4 Behavioral Biometrics

Schneier have some reminders about the possible implications of using biometrics extensively:

> "[B]iometrics work great only if the verifier can verify two things: one, that the biometric came from the person at the time of verification, and two, that the biometric matches the master biometric on file. [. . .]
>
> Biometrics are powerful and useful, but they are not keys. They are useful in situations where there is a trusted path from the reader to the verifier; in those cases all you need is a unique identifier. They are not useful when you need the characteristics of a key: secrecy, randomness, the ability to update or destroy. Biometrics are unique identifiers, but they are not secrets." [69]

Schneier's reminders does apply to physiological biometrics, e.g., fingerprint, facial features, and the iris. This was however written in in 1998. The category of behavioral biometric may not have been very established at the time. Behavioral biometrics can be practically secret to the human eye and confirmed coming from the user at the time of verification. It functions by collecting enough data points of a human behavior over time to, first, *enroll* by creating an initial master record, and later, *authenticate* or confirm the user by comparing the master record to a new recording [4]. For the human eye, the details of the uniqueness of human behavior can be quite concealed. Small behavioral details makes that person unique. Since behavior is tracked over a period of time (the time it takes to scan), it can also, with more certainty, identify that the user is actually present. Also, since behavior is tracked over time, this presents the options of having a 'secret' movement that is changeable, thus another of Schneier's arguments against biometrics may be questioned.

I related the ideas 'movement', 'drawing', and 'game' to behavioral biometrics, as they can potentially be that when performed with movement. These ideas also have the factor of 'what you know', meaning that they have the potential to change the user credential like a password. Voice recognition is also a behavioral biometric [56], and can be usable for particularly scenarios, e.g., in a phone call, but has a flaw for use in a login procedure, the user has to talk. This can potentially be awkward in social settings involving strangers, making it conveniently unacceptable for some users [7]. Authenticating by movement does have a similar issue as voice recognition; the user has to do a movement in public, which may be awkward. The question if this is an issue was further discussed in the second workshop, but I thought that movement was invisible enough, and also acceptable enough as a way of interacting with computers. These ideas were also very interesting suggestions in regards to expanding upon a 'cool' or 'fun' way of authenticating. In relation to 'cool', interaction by movement has a famous scene in the sci-fi movie Minority Report[1].

'Movement' can imply authentication by either how the user moves or what movement s/he does. Compared to 'dancing' and 'scanning the entire body', 'movement' has another interpretative advantage in that it may need 'less' of the body. It was mentioned during the workshop that 'dancing' was not wheelchair friendly. For the ideas 'movement', 'drawing', and 'game', I chose to focus on hand movement.

It has been recognized within psychology that the human brain easier recalls "visual information as opposed to verbal or textual information" [8, p. 3]. Graphical password schemes, among them 'drawing', has been widely studied [8], but have never really caught on. This may be due to that the ordinary PC supplements of mouse and keyboard have never been very well suited for drawing. With the coming of touch devices, graphical passwords may have found its platform. One authentication application for Android exists where the user draws simple geometrics — dot, line or circle — on an image of choice. And to authenticate has to choose the right image and redraw the dot, line and/or circle [74]. The suggested 'drawing' can imply authentication by either what the user draws, how the user draws — the behavioral aspect, or both. It also raises the question of where to draw, e.g., interaction with a touch device or motion sensors. Drawing has been cleverly applied for authentication on the Android platform [74]. With new technology, perhaps authenticating by drawing still has a chance of catching on. It can, however, require a level of fine motor skills or vision.

'Game' can imply authentication by how a users solves a game, which can incorporate the behavioral data points from movement and the result. I have not found any literature on using games as authentication.

[1] Steven Spielberg. Minority Report. In collab. with Philip K. Dick (short story) et al. June 21, 2002.

Behavioral biometrics works by recording behavioral data over time. That opens up for nice ways of combining it with a 'what you know' factor. In security literature there is normally a focus on how two factor authentication is more secure: "A common example of multi-factor authentication is the bankcard. The combination of a bankcard plus a [PIN] — two-factor authentication — is a better choice than a card alone because the card can be stolen and used, whereas a card that is password-protected cannot be used without knowing the secret" [56, pp. 2023-2024]. Todorov points out that "multiple-factor authentication is very likely to increase the time it takes for users to log in. Therefore, users may be resistant to using multiple-factor authentication mechanisms" [72, p. 19]. The 'movement', 'drawing' and 'game' ideas are in a way natural two-factor ways of authenticating — the confirmation of user depends both on something s/he is and something s/he knows. A behavioral biometric system must scan the behavior based on a persons movements anyway, why not make that movement count. Schneier points out the fact that a stable physiological biometric can never be changed and it is not a secret [69]. It may be an advantage to combine a behavioral biometric with a 'what you know' factor so the user can change his/her user credential, like a password.

3.7 Recap

From the critique phase the participants made it clear that the amount of passwords they had to manage were too many. It lead them to take short cuts like telling the passwords to friends if they were to tired to log in themselves, or using Facebook's login solution, even though they felt it wasn't secure towards their privacy. Facebook could disrespect their privacy by allowing services to post to their Facebook wall and that it was easier for someone to access applications they used because they had not logged out of Facebook.

The ideas of 'movement', 'drawing', and 'game' were chosen to be the main focus for the next workshop, both from behavioral biometrics being promising compared to its 'competitors' and from that the Leap Motion — chosen as a the possible technology to materialize the ideas — is something the participant can perceive as being cool and find as fun. Inspired by Jordan, instead of avoiding negative feelings from arising, or rather in addition to avoiding negative feelings, the direction of the design should aim to give the participants an experience of cool and fun, but still highlighting low-intrusion of the authentication method. From the fantasy phase the word ‘cool’ was used within a brainstorming where the participants fantasized about a sci-fi like direction of authentication. ‘Innovation’ is the sci-fi nod in Read et al.’s ‘cool’. The functioning of the Leap Motion in itself may tick off the boxes ‘innovative’ and ‘rebellious’. ‘Innovative’ since it is new technology that enables in-air, gesture based interaction, and ‘rebellious’ in being rule breaking, since technology like this has mostly only been seen in sci-fi movies. In an earlier research, Read et al. found that innovation and rebellion may be key aspects of cool [63, p. 1571]. Motion tracking through the Leap Motion for authentication may also be fun from being playful, active, and giving a feeling of sensation. Hassenzahl and Tractinsky asks if it is possible to design emotions or if designers should settle for establishing the context for emotion [28]. With the Leap Motion as technology, it may provide the context for emotions related to cool and fun.

Using the Leap Motion to possibly materialize a prototype would mean that this design process takes the direction of initially creating an authentication method for PC, since there are no similar technologies currently available for smart devices (though there are similar technologies in development for smart devices).

The second workshop was also to included a survey where the participants could rate some additional authentication methods. These authentication methods were ‘one-time pass code via phone’, ‘fingerprint’, and ‘facial recognition’.

3.8 Preparing for Workshop II

The next workshop took place three months after the first one. The preparations for the second workshop mostly consisted of discussing and reviewing the data, reading, reviewing design ideas, and sketching. Before choosing a method for the second workshop, I used the use-oriented design cycle (see Figure 2.1) to visualize where in the design process I was and where I had to continue. The first workshop had covered ‘understanding practices’ and ‘identifying needs and wishes’. ‘Describing requirements’ was done a lot in the discussion above, and would continue in the discussion of the second workshop. ‘Concretizing and materializing’ was started in form of the Leap Motion, but would need more detailed ideas in preparation for the second workshop. The second workshop had to further identify needs and wishes based on the concretizing of the Leap Motion ideas.

Because of choosing the Leap Motion as a possibility for realizing the ideas, I wanted to use it in the next workshop with the participants. Therefore I chose what I found to be a suitable method — Experience Prototyping (previously explained in Chapter 2). It also seemed like an engaging method, it just needed some more details for the participant's ideas to get the participants to discuss and brainstorm. From the ideas 'drawing', 'game' and 'movement', I further created small design ideas of user credentials that I thought could be realized on the Leap Motion platform. Sketches of the ideas can be seen in Appendix B, section Sketches. The ideas had to involve enough movement for it to theoretically be able to authenticate a user, but the ideas would also have to involve the user's chosen movement.

Chapter 4

Second Workshop: Experience Prototyping

This chapter presents the second workshop with its implementation of the method Experience Prototyping, the findings, and the discussion of the findings and how it helped me to proceed to a prototype. As the previous workshop the discussion of the findings were based on organizing data, identifying themes, reading, and writing.

4.1 Why This Method?

The aim of the second workshop was to explore the possibilities of a behavioral biometrics based authentication method combined with a 'what you know' factor, using in-air hand gestures materialized by the Leap Motion. Experience Prototyping felt like a 'natural fit' since I wanted the participants to experience the Leap Motion through use. Buchenau and Suri identifies three activities in the design process where Experience Prototyping is valuable: when understanding existing user experiences and context; when exploring and evaluating design ideas, and; when communicating ideas to an audience [13]. Where the two latter directly applies to this workshop. According to Buchenau and Suri, when exploring and evaluating ideas: "Experience Prototyping can provide inspiration, confirmation or rejection of ideas based upon the quality of experience they engender" [13, p. 431].

Date	February 26, 2015		
Purpose	‘Exploring the possibilities of a behavioral biometrics based authentication method combined with a ‘what you know’ factor, using in-air hand gestures materialized by the Leap Motion.’		
Method	‘Experience Prototyping’,	25 min total	5 participants split into 2 groups of 2 and 3, age 17-21

Table 4.1 Overview of the second workshop.

4.2 Implementation

As the previous workshop, it was not known how many participants that would be able to participate before the day of the workshop. For this workshop, five participants were able to participate. The participants partook in the workshop in groups of two and three. This was both for practical reasons for the other KULU design research done at the same afternoon, but also suited the method for this workshop. The fact that they would interact with a prop would make it more engaging for fewer participants at a time. The participants were between 17 and 21 in age and they all knew each other. The location of the workshop was at the Akershus University Hospital (Ahus). In the same room as the previous workshop, and as last time, before the workshop started, this room was also used to eat pizza in. The existing product, the Leap Motion, was used as a prop in enacting, along with the needed computer it depends on. For this workshop, the computer was a laptop. Though not intentional, the laptop did help set the setting for the workshop. The setting was to log in (somewhere) from a PC.

In the start of the workshop the group of participants were re-introduced to what happened in the last workshop; their critiques of passwords and Facebook login, their utopian ideas, and how they had been reviewed. Then I explained behavioral biometrics, why this workshop looked at this particular way of authenticating, and how some of their ideas from the Future Workshop could be related to that. The workshop moved on to introducing the Leap Motion as a technology that could realize these ideas. The participants were allowed to play freely with the Leap Motion together for approximately five minutes. Each participant tried it some of the Leap Motion's introductory applications (see Figure 4.1). This was to create tacit knowledge of how it felt to use, so they later in the workshop could provide more valuable design feedback and brainstorming. After that they were shown a short video of different use cases and applications for the Leap Motion to further understand its potential.

Then we moved on to exploring the possibilities within an authentication method that used hand movement. The ideas from the future workshop's fantasy phase that were the inspiration, and could be related to this technology, were 'movement', 'drawing', and 'game'. From the basic scenario of having the participants imagining that they were logging in, the participants would enact how they would log in by hand-movement, 'hand-drawing', or gaming with their hands. For each of these ideas they were shown some inspirational images and sketches (my sketches) to how the ideas could work in relation to the Leap Motion. I had planned three ideas of design that they could explore within if they wanted, or explore other ideas if they were to come up with something:

- Using a letter from the alphabet as your 'password'.
- Using a personal movement, e.g., something from a hobby, as your 'password'.
- Using interaction with a game, e.g., Fruit Ninja[1] and a similar idea with balloons, to see if the participants would want to further elaborate on the 'game' idea.

The participants were allowed to freely express themselves during the enacting to get a free flowing conversation going on all topics of interest for both parties. I had also planned some questions of interest for the design and research.

4.2.1 Survey

At the end of the workshop the participants answered a short survey. The survey can be seen in Appendix B, page 106. I used the survey as a way to get the participants' opinions on some of the other good ideas from the Future Workshop. One point of using a survey that I did not take fully into consideration was that it could give the participants a

[1] Fruit Ninja is a game for touch and motion based platforms where the player slices fruit with a 'blade' controlled via touch or in-air motion gestures using a finger.

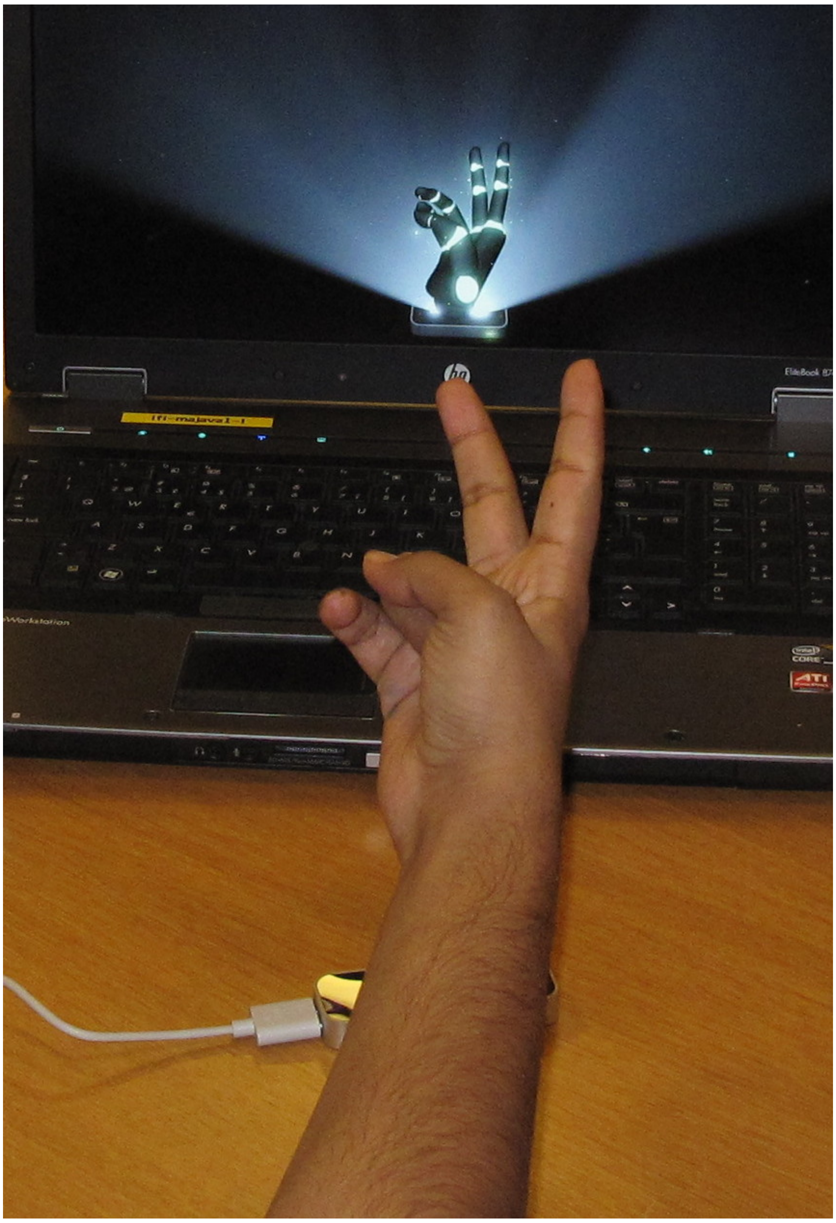


Figure 4.1 A participant trying the Leap Motion.

chance to be more anonymous. They only wrote the ID number they had during the workshop — that was to know their age and gender — but a full feeling of anonymity was difficult to pull off in reality since they were only five participants for this workshop. Their answers also reflected opinions they had shared during the workshop. Being more anonymous can make people more comfortable towards being fully honest, but from the answers it did not seem like they cared too much about full anonymity. They happily told me the ways of authentication that we had discussed and how other ways could possibly be better, which was good to see.

4.3 Findings

Same as the previous workshop, all of the participants knew each other and several of them seemed to be good friends, which gave good ground for a good atmosphere of participation. One by one each participant tried the Leap Motion while the other watched. All of them praised it as 'fun', 'cool', and 'sci-fi'. There were some initial problems with were to place their hands so the Leap Motion would register them correctly, but that did not bother their engagement and fascination. "Is this pretty new?" a male participant (age 21) asked. None of the participants had used a Leap Motion before. From a conversation with group 2 during the workshop:

Girl 4 (age 18)	"This is so cool! This is so cool!"
Girl 6 (age 19)	"It is fun."
Girl 4 (age 18)	"It is strange that one can be so fascinated by stuff like this."
Girl 1 (age 17)	"Yeah, it was fun."
Girl 4 (age 18)	"It is something you can sit and do for a very long time. It's a bit like what you see in sci-fi movies.'
Me	"Yes, 'Minority Report', have you seen it?"
Girl 4 (age 18)	"Yeah, that's the one I was thinking about."

Figure 4.2 Still image from Minority Report.

At the end of the workshop, group 1 concluded that authenticating by hand movement with the Leap Motion was very good compared to other ways of authentication, i.e., face recognition, fingerprints, and iris recognition.

4.3.1 Authenticating by One Movement

The participants were asked, if they were to log in with one movement, what would that movement be? One participant of group 1 suggested signature writing, but they soon agreed that it would be too detailed movements and difficult. The other participant suggested that she would rather pretend to give a 'fist bumb' or draw a circle — where we in turn concluded that it must have some wiggle room for accepting the user credential. From group 2, there were no answer to this open question, and I just moved on to the next more specific question.

4.3.2 Authenticating by Drawing a Letter

The next question was what they though about drawing a letter in the air as authentication. I also explained a little more about how it technically would authenticate. Since machines can detect movement in more detail than humans, it was the finer details in the movements that would confirm with an amount of certainty that it is the right person, and the movement pattern the person has as a 'password' would confirm the last bit that it is that person. In group 1, drawing a letter in the air brought a concern of *shoulder surfing* — a security threat where the attacker observes a person that is using his/her secret in a knowledge based authentication, e.g., observing someone typing their PIN at an ATM [72]:

> “That I write an ‘A’ like this, in cursive [she write an ‘A’ in the air] [. . .] What about just bringing two fingers together, that it was just as simple as that. [. . .] If I stand and write an ‘A’ like this [she writes an ‘A’ with big motions in the air], then everyone would see it. ‘Hi hi, everyone. ‘A’ is my password.’ If I only do this [she snaps her fingers], people probably wouldn’t notice.” (Girl, age 20)

In group 2, I asked if they were to use a letter for logging in, would that be simple, fun, or too much:

Girl 4 (age 18)	“Fun.”
Girl 6 (age 19)	“Fun.”
Me	“Yeah. And it’s something you would want to do?’
Girl 1 (age 17)	“Yeah.”
Me	“Instead of using passwords for example?’
Girl 1 (age 17)	“Yes, much rather.”

4.3.3 Authenticating by Personal Movement

The next design idea we moved to was using a movement that is personal to you, as a movement for logging in. In group 1, one participant used to play handball, and suggested to use one of those movements for logging in since they are were very natural to her. The other participant in group 1 played soccer, but the Leap Motion is meant for hand movement. In group 2, one participant played guitar, which could be a suitable movement.

4.3.4 Authenticating by Drawing

When discussing how to use drawing as authentication, group 1 found drawing to be to fiddly in authentication. One participant in group

2 however, found it very interesting, and it seemed like she was into drawing. When I asked her if drawing would not be difficult to repeat (I envisioned a detailed drawing of a house for some reason)? “A simple symbol or something, and it works”, she (age 18) said.

4.3.5 Authenticating by Gaming

Group 2 was very interested and thought it would be fun to use a game as authentication. They did not have any examples of game mechanics, but examples of that you had to reach a specific score, for example your lucky number, and that it had to be a quick moving game. Group 1 where focused on if they were tired and had to play a game to log in, it would be too exhausting. For this reason they thought it would have to have a fallback user credential.

4.3.6 Other Forms of Authentication

During the workshop other form of authentication were sometimes brought up in the discussions.

Voice Recognition: In the analysis or discussion of the ideas from the Future Workshop, I made the assumption that voice recognition has a barrier of use for many people, for example, if you have to talk to your computer in middle of class. Voice recognition was brought up in the second workshop were it seemed like the participants agreed with me, joking that they would have to whisper to their computer and it would not hear you. Another participant saying that ‘Siri’ on the Iphone did not understand him anyway.

Face Recognition was something group 2 thought was cool. I asked if they thought it could feel privacy invading in any way, but they did not feel that.

Fingerprint Authentication: A participant of group 1 felt fingerprint recognition was the easiest to use.

Iris Recognition: The other participant of group 1 thought iris recognition was very interesting in regards to accessibility — that she thought everyone could use it — but also that I mentioned that it is one of the most stable biometrics we know about. She also thought behavioral biometrics with hand movement was a very good and usable idea, but if a person for a period had a cast it would be unusable, which can be correct.

4.3.7 Survey

The first question on the survey was if they would have liked to log in using the Leap Motion. (The survey can be seen in Appendix B, page 106). They could rate it on a scale of five, from ‘dislike very much’ to ‘like very much’. Four of the five participants rated it ‘like very much’, and one rated it ‘like’ as can be seen in Table 4.2. The next question was why, where the participant that rated it 4 answered: “Liked it because it is the first time I have seen it. Can be a bit annoying to use on a bad day”. Another participants answered about the same, even though rating it 5. This participant also mentioned how fun it was. The three last answers also focused on how fun it was, and that it was cool, and one writing: “Because everything sci-fi is cool!” Two of them thought it seemed very easy to use compared to passwords.

The third question was about three other ideas from the Future Workshop. The ideas were to be rated in the same way as the Leap Motion, and why they rated as they did. The ideas to rate were ‘one-time code to phone’, ‘fingerprint authentication’ and ‘face recognition’. Table 4.2 shows the ratings of all the participants. Three participant rated ‘dislike very much’ for ‘one-time code via phone’. For reasons, two wrote “boring”, and one wrote “tiresome”. The one ‘neutral’ rating was reasoned with: “A bit over used, easy to hack”. One rated it ‘like very much’ and wrote: “Quite simple”. Fingerprint authentication got four ‘like’ with the reasons “good idea” and “simple”. One participant gave it top rating and wrote: “Best idea I think. Simple”. Face recognition was the second most like authentication. One wrote “simple and fun”, but one wrote that the eye particularly was interesting — seemingly not necessarily the face. The same participant who really like fingerprint authentication rated ‘face recognition’ as ‘like’, but writing: “Totally OK. Less simple”. Which I assume is especially less simple that fingerprint authentication, though he also felt that it was less simple than ‘hand movement authentication’ and ‘one-time code via phone’.

The last question on the survey was simply ‘Comment?’. Only two participants chose to comment. The same participant that was interested in iris or eye recognition wrote: “Liked the idea of Leap Motion and movement as password. Also would like to see eye recognition”. The last comment was: “Drawing and movement was coolest”.

	Dislike very much	Dislike	Neutral	Like	Like very much
	Five participants' ratings:				
Leap Motion (hand movement)				**x**	**xxxx**
One-time code via phone	**xxx**		**x**		**x**
Fingerprint				**xxxx**	**x**
Face recognition				**xxx**	**xx**

Table 4.2 All of the five participants' ratings from the second workshop for each of these authentication methods.

4.4 Discussion

In relation to the Leap Motion and the ideas, both groups mentioned 'fun' and 'cool' several times. Perhaps part of the fascination for the Leap Motion can be explained in how new it is. None of the participants had used it before, but as mentioned, the Leap Motion falls under innovative and rebellious in Read et al.'s cool design guidelines [62]. This points to that these guidelines were relevant as 'cool' for the teenage participants of this project. And in relation to fun, the use of Leap Motion is active and playful. Compared to the other authentication methods included in the survey, the Leap Motion came out on top.

Moore explains how 'cool' has for some decades been associated with teenage culture after it replaced the word 'swell', and can be seen as a teenage 'knowingness' of their own culture (as cited in [47]). I was surprised that they used the same word that has been used across several generations and countries to express themselves. It should be considered that they may not be contributing it the same meaning or value as other generations or social groups. Just because the participants said 'cool' does not mean a design then is accepted into the current teenage culture (or 'knowingness'). The term 'cool' can for the actual teenagers (e.g., the participants in this project) just be a word to express that something simply is cool. And perhaps what was perceived as cool for teenagers 15 years ago has a different word now. There are many discussions on the implications of the word 'cool' and its meaning [47]. For this workshop it generally seemed like 'cool' was used to express their positive enthusiasm. They were enjoying the technology and it engaged them. ‘Fun’ and ‘cool’ may have been synonymous to several of the participants in this context of use — it was both fun and cool to use the Leap Motion — but one participant was very clear on that everything sci-fi was cool.

4.4.1 Design Considerations

From the first design suggestion we looked at — generally using a hand movement to login in — there were uncertainties from the participants of how precise they needed to re-perform the hand movement to log in. A high fidelity prototype of a hand movement authentication method must have a fined tuned wiggle room of user credential acceptance.

The feeling of being secure was important for the participants. One participant explained: “If I stand and write an A like this [doing big hand gestures in the air], then everyone would see it” (Girl, age 20). Theoretically this would not be enough for another person to log in as you, but it could be an uncomfortable feeling — the feeling of it not being secure. And the feeling of being secure should after all be important in the user experience of a security element. The methods ‘one-time code via phone’ from the survey was considered ‘easy to hack’ by one participant, as was passwords and Facebook login from the critique phase of the first workshop.

Two participants raised concern about the ‘fun’ in authentication when they were too tired. People should have the right to have the experiences they need and desire rather than having experiences “thrust upon them by poor designs” [7, p. 99]. This points to McCarthy and Wright’s highlight of the need to take an holistic approach to UX (as cited in [7]). Experiences have to be understood as a whole and cannot be broken down into their constituent parts since experience lies in the relations between the parts [7].

4.5 Reflection

The second workshop did not produce the same amount of findings and discussion as the first workshop. This may have been to the fewer participants, but also to where this project was located in the design process. Coming from a divergent first workshop, in retrospect — the second workshop took the design process into a more convergent part it. Divergence creates more information and options, while convergence focuses on specific solutions [44]. As Madden explains, there two ways to organize and find meaning in qualitative data: “[1] the idea that data consists of facts that will speak for themselves and [2] that data consists of information that we actively create meaning from as a consequence of our own intellectual and theoretical predispositions” [48, pp. 139-140]. For this workshop, there were more findings that related to the first way of interpreting; findings that ‘spoke for themselves’. “Convergence creates a deeper understanding and a more detailed and narrowly focused proposal” [44, p. 29].

Chapter 5

Prototype: Pass-Gestures

This chapter presents the latest iteration of the design of an authentication method based on the findings of this thesis. This prototype is mainly of the user credential of an authentication method, which I have called a pass-gesture. The process of authentication consists of two distinct phases: (1) identification and (2) (actual) authentication [72]. *Identification* provides the system with the user's identity. This identity is typically provided in the form of a user ID. *Authentication* is the process of validating a user identity. To ascertain that an actual user can be mapped to a specific abstract user object in the system, the user must provide evidence to prove his identity to the system [72]. This evidence is called the *user credential* and it incorporates the *authentication factor*, or factors. The base categories of authentication factors are 'what you have', 'what you know', and 'what you are'.

5.1 The User Credential: A Hand Gesture

The user credential of this thesis' authentication method is both a 'what you are' and 'what you know' authentication factor by being an in-air, hand gesture. The in-air hand gesture is visioned to be tracked by the precise motion tracking technology Leap Motion (but can probably be imagined to be realized with future similar technology for a diverse range of operating systems and devices). The Leap Motion creates 8 cubic feet of interactive, 3D space where it tracks finger movements as well as bigger hand movement [43].

The 'what you know' factor of this authentication method is a specific hand gesture that acts as a password in the sense that the user chooses a specific hand gesture him-/herself. So, from the role the hand gesture has, it could more precisely be called a 'pass-gesture' instead of a password. The 'what you are' factor of this user credential is how a hand movement is a behavioral biometric. The behavioral aspects of movement can be said to be the more invisible and finer personal details that are part of a person's movements. The finer details of movements are possible to track with detailed motion tracking devices like the Leap Motion. Technically, parts of the behavioral aspect of this user credential may require a very scientifically developed and fine tuned set of self learning algorithms, which is literature that is not within the scope of this thesis. The more approachable parts of behavior, e.g., how a specific user performs his/her movements in a certain way, are quite possible to develop. For example, if the pass-gesture included a circle, a behavioral aspect could simply be that the user 'draws' the circle in a fixed direction (see Figure 5.1). It could also be more unique details like how the user's fingers are placed in a specific way, or how they unconsciously moves together with, and within a hand movement.

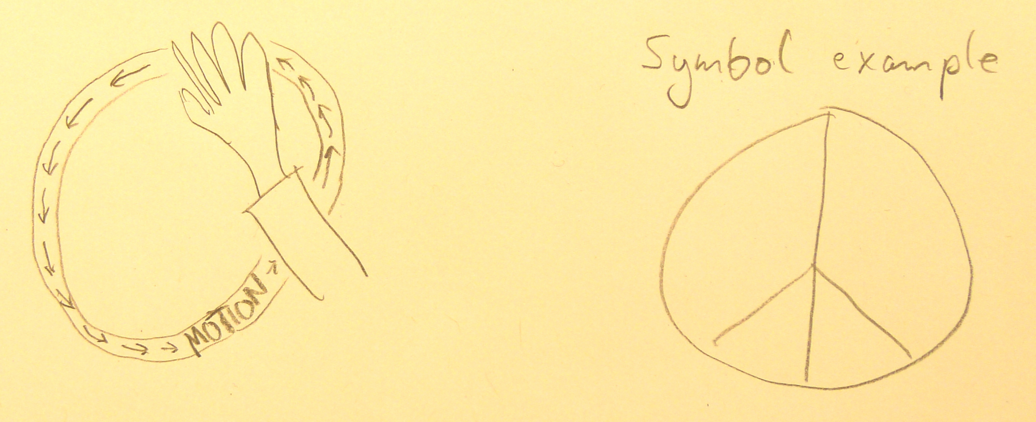
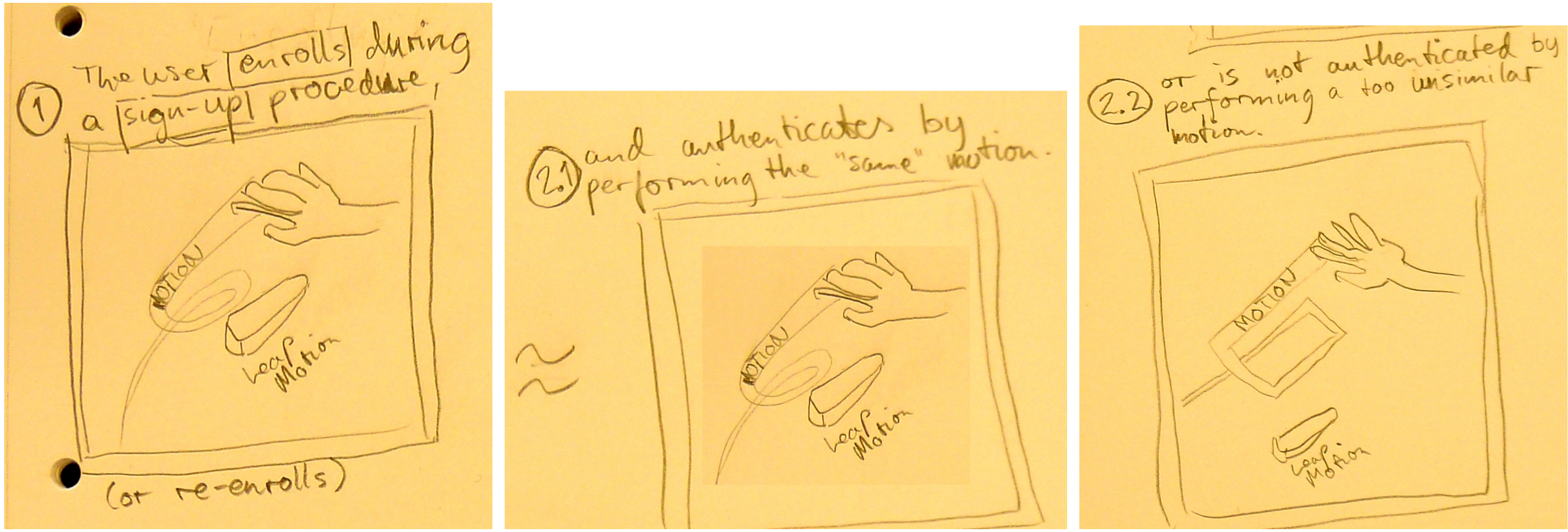


Figure 5.1 A simple behavioral aspect and a symbol as a gesture that includes a circle motion.

In a biometric authentication system there are usually two stages of operation: The enrollment stage and the authentication stage (see [4] Figure 5.2). The gesture is *enrolled* when the user performs his/her gesture the first time. While the user performs his/her chosen gesture, the Leap Motion tracks and records the gesture to a master record. The enrollment is done during a sign-up procedure, or when the user wishes to 're-enroll' the gesture. The authentication stage happens at a later stage; during login, the user performs the same gesture as enrolled and the Leap Motion checks the authenticity of the user by comparing with


1
The user enrolls during a sign-up procedure,
MOTION
Leap Motion
(or re-enrolls)
2.1
and authenticates by performing the "same" motion.
≈
MOTION
Leap Motion
2.2
or is not authenticated by performing a too unsimilar motion.
MOTION
Leap Motion

(a) 1. The user enrolls during a sign-up procedure…

(b) 2.1. …and is authenticated by performing the 'same' gesture.

(c) 2.2. …or is not authenticated by doing a too dissimilar gesture.

Figure 5.2 The stages of operation in the authentication method.

the master record. As the participants pointed out, the authentication stage has to provide sufficient wiggle room to avoid false negatives.

5.1.1 Choosing a Pass-Gesture

The range of hand gesture that the user can choose as pass-gesture are quite endless, only it can not be too simple since there has to be enough movement in the gesture to make it unique enough to authenticate a person. What 'too simple' actually is requires testing in relation to the algorithms that are used in the programmed code of a high fidelity prototype. Like passwords, this user credential thus has some requirements; the gesture can not be too simple. Unlike passwords, this is known before this method is in use. And it should perhaps be incorporated into the design to avoid a difference in requirements for each implementation, as has been seen in password based authentication. The requirements of a pass-gesture does raise the question if it will fall into the same use issues as passwords has done? The main argument against this is that behavioral biometrics works by recording data points from behavior within a time frame — in this scenario the data points are several, both of hand and finger movements at the same time in a 3D space. In future development of behavioral biometrics systems, harnessing all possible data points will only improve, so the requirements will ultimately decrease over development time. Another argument is the same argument that graphical passwords have used, a drawing is easier to recall than a password [8].

The design has to explain the requirements for the gesture in a very comprehensible way. From the second workshop 'drawing a simple symbol' was a suggestion from one of the participants and can be used to create an approachable mental model for users. A person's mental model represents how s/he understands and knows something [7]. "*[M]ental models*, the models people have of themselves, others, the environment, and the things with which they interact. People form mental models through experience, training, and instruction" [54, p. 17]. To use a simple symbol as hand-gesture is easy to explain to new users and will perhaps provide a simple mental model, but it does require that the person can actually think of a simple symbol. Based on the chosen symbol, this can, however, be identifiable from shoulder surfing. The user can of course choose to draw the symbol with his/her fingers. Opposed to drawing a letter in the air, drawing a symbol has a lot more possibilities. Even a letter can be a symbol. In the paper "AirAuth," Aumi and Kratz conducts a study where 10 participants came up with in-air hand gestures they would be willing to do to authenticate Aumi and Kratz (see Figure 5.3). Their results are basically simple symbols.

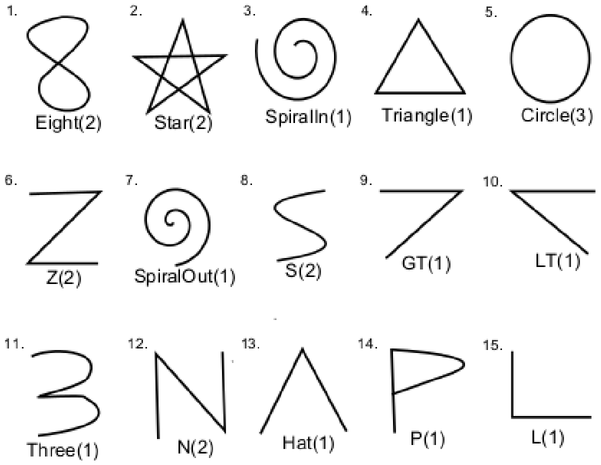


Figure 5.3 Hand gesture 10 participants thought of as simple from the paper "AirAuth" [4].

The Leap Motion utilizes the PC screen to, e.g., show a replication of the hand while it moves (see Figure 5.4), and utilizing the screen interface in the right way is key to providing a good mental model for the user. It must also support and perhaps extend the 'cool' and the 'fun'. Biddle et al. writes how it has been recognized within psychology that the human brain easier recalls "visual information as opposed to verbal or textual information" [8, p. 3]. So for the symbol to be easily recalled it may require some visual information on display to what the user 'drew' during enrollment.

Section 7.3 The Way Further summarizes the way further for a final design.

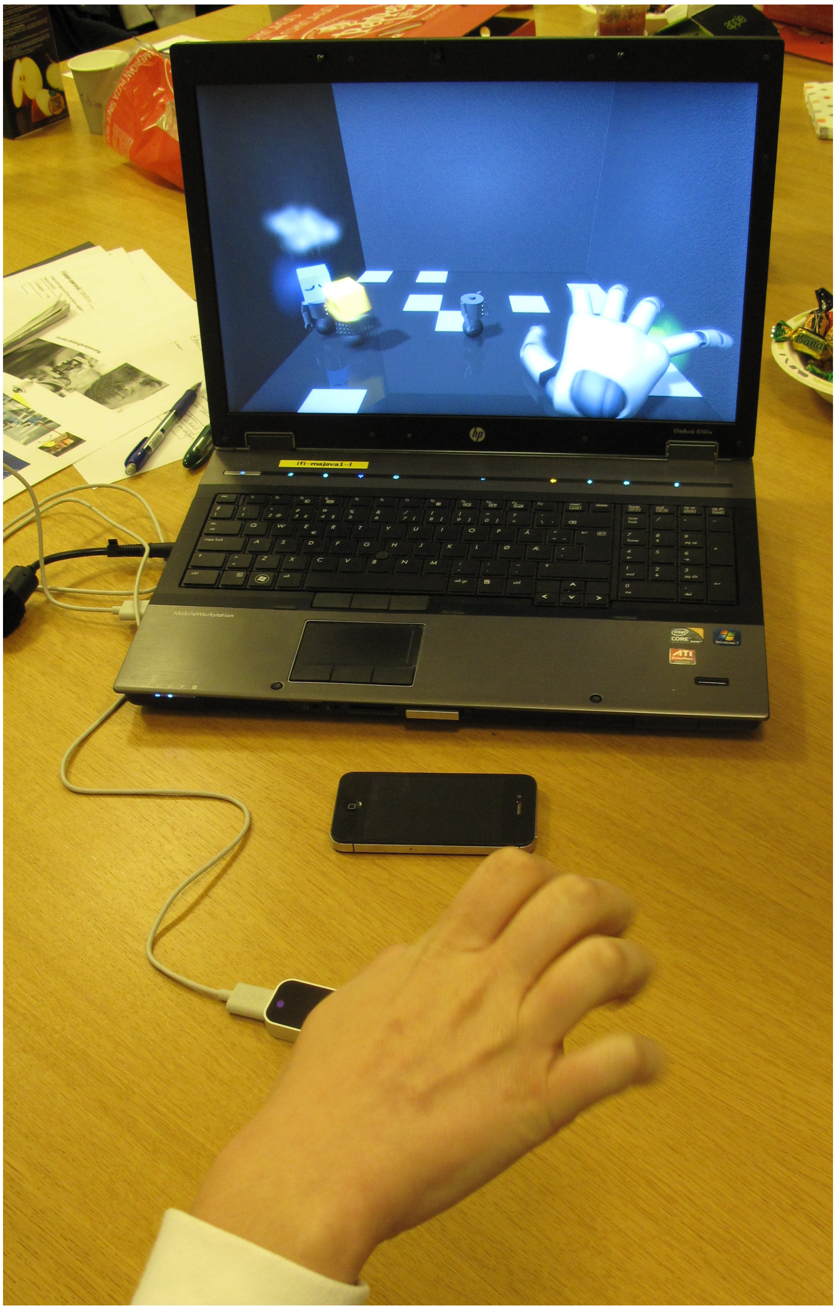


Figure 5.4 A participant playing with the Leap Motion during the second workshop.

Chapter 6

Discussion

This chapter will put the findings of this thesis into the context of the background presented in Chapter 1 Introduction.

In Feenberg's model to examine the theories of technology and society there are two dimensions: (1) neutral versus value-laden technology, and (2) autonomous versus human controlled technology (as cited in [60]). Verbeek explains how technological artifacts have values by explaining their mediating roles within the relationship between human beings and reality [77]. In this role technological artifacts direct human beings by how they shape the intentions of human beings by the artifacts' 'built in' mediations [77]. As explained in Chapter 1 Introduction, authentication has a mediating role in the relation between human beings and reality by being a gateway to digital participation in society. From this role, the importance of usable and accessible authentication methods supports a need to broaden the design approach the Norwegian Government has chosen as the ideal approach to design technology that supports an Information Society for all. This design approach is Universal Design (UD). By finding built in mediations that supports an Information Society for all, a true universal way of authentication can be designed.

According to Redström, a PD "process enables the emergence of values and definition of use, while the artifact (product or service), in its different stages of development, enables the exploration of those different definitions of use" (as cited in [76, p. 3]). In the design process certain values emerges and these values are 'built into' what is designed — the process and the product are of equal importance [76]. According to van der Velden and Mörtberg, during a PD process the designers and co-designers take design decisions that implicitly and explicitly inscribe values into the final product [76]. "The importance of this process lies in the fact that technology mediates the behavior of people" [76, p. 3]. The prototype of this project was the product of a PD process where certain values where 'built into' the prototype. These values emerged during the process from the participants' opinions and further from my interpretations.

The participants, and also co-designers of this thesis were long-term teenage patients, though healthy enough to possibly participate in the workshops. I say possibly, because I never knew beforehand who would be able to partake in the workshops. The participants also had diverse health challenges. The differences in the challenges the participants had and the uncertainty of who would participate, directed this thesis to take a broad approach towards the accessibility problem of authentication. Still, this group of participants may be well suited to be a part of the future direction of authentication design. Passwords and PINs have mainly conceptual challenges of use. As patients with long-term health challenges, they have evidently experienced the memory load connected to password use. As one participants said, sometimes she was so tired that she had to share particular passwords with friends so they could help her log in, thus she felt that password based authentication was not secure. Other findings that reflect this particular user groups are how dancing was not wheelchair friendly and how one participants suggested to log in by scanning scars. Values that emerged during this design process that are related to the participants being who they were, may be apparent in the resulting prototype. It has a focus on simplicty in its interaction. The teenage side of the participants are definitely also present in the cool and fun aspect of the prototype.

From the first workshop, I interpreted the participants ideas for alternatives to passwords to a very usable authentication method with low intrusion, i.e., efficiency and high utility. The reasons for low intrusion are easy to understand with the memory load related to the password and PIN based authentication. The participants also suggested ideas that engaged them. Here I interpreted the ideas as engaging through the UX design concepts 'cool' and 'fun'. It was made clear in the second workshop that some participants were concerned that usability would be neglected for the fun aspect. Usability in HCI has been developed over a long time, and not out of thin air, so it should come as a no surprise that a design often has to think about usability first.

The participants were also interested in maintaining security. From the first workshop a participant suggested several fingerprints as the user credential, as more fingerprints would make an authentication method more secure. Maybe this was a critique to the security of the

Iphone's fingerprint based authentication, which the same participant felt was the simplest way to authenticate. In the second workshop, one participant thought that using easy observable hand gestures would make it insecure against shoulder surfing. An authentication method has to not only be secure, but feel secure.

6.1 Social Construction of Technology

The field of science and technology studies (STS) is an "interdisciplinary field concerned with the study of how scientific and technological changes intersect with society" [60, p. 51]. One approach within STS is the social construction of technology (SCOT) approach. They argue that a technological object can acquire different uses and values according to the social context it is placed in [60]. Within SCOT four key terms help to understand the interplay between design, technology, and society: the relevant social group, interpretive flexibility, closure and stabilization, and wider context [60]. According to Bijker, *relevant social groups* are important due to their influence in attributing meaning to an artifact (as cited in [60]). "Without the necessary societal support, a new or existing technology can fail to be viewed as useful within a respective group, causing both new and older products to be viewed as obsolete" [60, p. 51]. *Interpretive flexibility* describes how artifacts are not neutral, their meaning emerges in a socio-cultural context [60]. For Pinch and Bijker what this means is "not only that there is flexibility in how people think of or interpret artifacts but also that there is flexibility in how artifacts are designed" (as quoted in [60]). *Closure and stabilization* describes how, first, the moment in the cycle of design when the relevant social group has reached a consensus of what the tool is all about, and, second, when stabilization is reached, the tool has been assigned a very specific use [60, p. 52]. The *wider context* describes how "the sociocultural and political situation of a social group shapes its norms and values, which in turn influence the meaning given to an artifact" (as quoted in [60, p. 53]).

According to Winner, critics of SCOT have argued that its supporters spend too much time studying the development and social construction of technology, but disregarding the social consequences (as cited in [60]). Winner presents another critique in how SCOT gives importance to some groups over other groups, the result is overlooking groups within society that have no input in approving a technology or that suffer from the social consequences of that technology's selection (as cited in [60]).

I will use SCOT to look at how the findings from this thesis may affect user-authentication or its context, and try to not forget the critiques Winner mentions.

6.1.1 The Current Context of User Authentication

From the current position of user-authentication in society, its design, and the changing of that design I see two relevant, broadly defined social groups that has shaped the current meaning of authentication (with a focus on password based authentication) in society. The first group consist of those that develop web-based ICT. This group is on a global scale and consist of several organizations, companies, governments, and even individuals. They are important because of their interpretation of password based authentication as the standard form of authentication. Without sufficient support from this group for a better form of authentication, new methods of authentication will probably not see the necessary investment of cost and time to challenge password based authentication.

This group is also important from how their interpretation, closure and stabilization of user-authentication enabled online identities for users, which in turn became a propeller for a next generation of web-based ICT. The wider context of user-authentication has been shaped by this meaning it got from the first group. The wider context I will focus on, is shaped by how authentication is connected to what became the next generation of web-based ICT and also to how the use of the Web normalized in more parts of society (which is still happening, e.g., through eGovernments). The closure of authentication made it follow along as an important mechanism in the web-based ICT that is a big part of the Information Society. The wider context of user-authentication is how it is a gateway for digital participation in the increasingly digitalized society. As Winner reminds us of the politics of artifacts by analyzing 'racist' overpasses (as cited in [77]), positioning authentication in a wider context highlights the importance of an indiscriminating authentication method.

The second social group is those who 'suffer' from user-authentication's bad design. This group can include people from the first group, and it does. Some people in this group suffer more, but to generalize, it is the group of all end-users of web-based ICT. This group interpret password based authentication as 'in the way'. It is a barrier to get past. Passwords are just not meant for the widespread use it have today through the Web and smart devices. At the same time as being a barrier, many users seem to accept, or deal with the fact that passwords are a part of everyday ICT use, but they often deal with it by adapting a neglecting perception of it as a security measure — compromising security. In computer security, the human user is often referred to as the weak link in a computer system [67]. This influences the wider context by compromising the security of the workplaces of the users.

6.1.2 A Future State of User Authentication

Norman argues that the more secure you make something, the more people will circumvent it [55]. For example password based authentication in computer security has been made more secure over time by applying different requirements. Behavioral biometrics have the potential to be very secure without adding more stuff to it. Since a hand gesture may include many data points, the potential for making it secure is mainly in improving the technology, not the user credential, and low intrusion both makes it usable and accessible. Usability is an aspect that has been said to be lacking in computer security. Usability has been improved in the context around passwords, but the user credential itself is not very usable. Password and PIN based authentication is just not meant for the ubiquitous computing we are seeing, where computers and the Internet are used everywhere. Improving usability and accessibility of the user credential is the first step in re-establishing user-authentication as security measure for the users themselves. It must be efficient and have a very high utility to fit in with how societies have become increasingly digitalized.

Sasse and Flechais claims that users will always think that even a very usable security system is a barrier [67], but perhaps this claim did not considered adding concepts from UX to an authentication method. A user experience that generates positive feelings and engages the user, may be a missing link to change users' circumvention of security. This will in turn improve security. Norman primarily blames bad design for why users circumvent security [55], others have blamed on insufficient user training in security procedures [22]. Draper arguments for UX as a design aspect that can improve learning [21]. In summary, for the first social group, low-intrusion and inclusion of UX concepts in authentication design may make user-authentication not to be a barrier and engage users. And as a result, the users may value authentication as the security measure it is, which may improve security for both end-users and their workplaces.

The biggest challenge, apparent from applying the SCOT perspective, is how to actually replace passwords. The support of the social group that consist of those that develop web-based ICT must be had. It may be wrong to say ‘support’, this group may perhaps just have to feel a general pressure from other social groups — that represents the users — to start replacing passwords. The pressure may also come from within. If one powerful actor upgrades the authentication methods its connected to, affectively another actor within this group may be forced to so too, and then another, and so on. A domino effect.

The design process of this thesis has not been bound by how ‘usability’ and ‘accessibility’ are traditionally defined in HCI, but was directed by the co-realization that happened together with the teenage patient co-designers. An argument for the possible importance of this: to further support future user-inclusion in the evolving Information Society, there is a need to widen the definitions of how something is universally designed to more than standardized guidelines. In relation to the wider context — to ensure that authentication as a gateway is accessible — looking outside of standardized ways of accessible design may further support an indiscriminating user-authentication. Since UD is the precondition for accessible ICT, perhaps the definition of UD should be broadened. And perhaps that could generate a domino effect.

Chapter 7

Conclusion

This chapter summarizes the design process and the findings, and describes the contributions of this thesis.

7.1 Design Process and Findings

The main research interest of this thesis was formulated as a design aim: "To design a user-authentication method that is usable, accessible, and designed with and for teenage patients." To reach this aim, Participatory Design (PD) was chosen as a design methodology and long-term, teenage patients were participants and co-designers. The design process was not bound by how 'usability' and 'accessibility' are traditionally defined in HCI, but was directed based on the co-realization that emerged during two workshops together with the teenage patient co-designers. The first design workshop was a Future Workshop were the participants criticized passwords and fantasized about alternative ways of authentication. All the eight participants of the first workshop agreed that they did not like to use password based authentication since there are so many passwords, they are hard to remember, and they are insecure. The participants suggested many highly usable biometric based methods as alternatives to passwords, but what seemed to be the most engaging suggestions for and by the participants were those that had non-instrumental, user experience (UX) aspects.

The post-workshop discussion of the first workshop focused on how usability and the UX concepts of 'cool' and 'fun' could be incorporated into existing user-authentication concepts. This directed the design process towards a novel way of user-authentication — a behavioral biometric based authentication using hand gestures. My supervisor suggested that I looked into using the Leap Motion — being a next generation motion tracking technology, it could support the design of an authentication method that used in-air hand gestures. The Leap Motion was used as a prop in the second workshop to give the participants tacit knowledge through 'experience by doing'. The method for the second workshop, Experience Prototyping, helped me explore and evaluated design ideas based on my post first-workshop discussion and work. The participants were generally very positive of the design direction, and from their tacit knowledge they imagined how authentication with in-air hand movement could work.

From my interpretations of the second workshop I derived three design aspects to include in the next step of the design direction: enough wiggle room to repeat their hand-gesture 'passwords' without false negatives; a secure feeling — especially feeling secure from 'shoulder surfing', and; that the 'fun' user experience does not feel forced, i.e., the relevant usability can never be compromised. The need to take an holistic approach to UX became apparent. "[E]xperiences have to be understood as a whole and cannot be broken down into their constituent parts, because experience lies in the relations between the parts" (as cited in [7, p. 99]).

The final prototype of this thesis is the pass-gesture user-credential to be used in an authentication method, where the behavioral biometric of a hand-gesture acts as a password, hence the pass-gesture. The pass-gesture both incorporates the authentication factors of 'what you know', but also of 'what you are', which is the behavioral aspect of the gesture. The direction of the prototype was based on the opinions of the co-designing participants and my interpretations in the after work. The final prototype has 'built in' values that emerged during the PD design process, both values for a more usable and modern-worldly friendly authentication method, but also a teenage engaging design that is cool and fun. The prototype is not perfect. For example, it is not a truly accessible design, as a participant pointed out, if you are wearing a cast, authenticating with a hand and finger based gesture will be difficult to do.

7.2 Contributions

Frayling identifies three approaches to how research and design relates: research into art and design, research through art and design, and research for art and design [24]. This thesis may seem to have had an approach of *research for design*, where the values that emerged in the process are now “embodied in the artefact” (or prototype) [24, p. 5]. But the design process of this thesis has mainly had an approach of *research through design* where communicable knowledge was the main focus.

In the book *Thoughtful interaction design*, Löwgren and Stolterman writes about what makes a ‘good design’ — it has to be evaluated in relation to situation, intentions and expectations, societal laws, regulations, agreements, and contracts, and in relation to ideological considerations such as democratic, cultural, and environmental ideals — good design is not a simple definition [44]. Password and PIN based authentication does not longer fit in with how societies have evolved. The memory load they generate does not support the further digitalization of Information Societies from new digital media, ubiquitous computing, and the expectation of citizens’ digital participation from public and private sectors. Still, passwords and PINs are considered universally designed by the requirements UD is regulated by in Norway. In computer security, the human user is often referred to as the weak link in a computer system [67], but it is pretty obvious that it is bad design that is the weak link. This thesis has explored possible alternatives to passwords with teenage patients by broadening the usual approach to accessibility and usability. And based on how they are tech-savvy teenagers with a unique understanding of technology in society, the resulting authentication method may be more adapted for the modern world, improving security and the access to participate in society.

The users’ own design opinions on user-authentication has been the focus of the design process. User-authentication is a technology that previously barely has had the users’ opinions. Usability is said to have a lack of understanding within the field of computer security, and usability clearly was a wish and a need based on the participants’ opinions, but also a UX aspect. Later, the need for an holistic approach towards the design became apparent. Both usability, accessibility, cool, and fun had to be considered against each other in the design process, and also an aspect specifically related to a security measure; the user wants to feel secure. The result of the design process was a user credential called a pass-gesture, a name that hints to its potential of replacing passwords as user credentials.

Teenagers obviously have grown up in a more technological world, and based on the participants’ design opinions on user-authentication, they evidently have a lot of input for how societies more efficiently can co-exist with digitalization. In the case of user-authentication; efficiency and high utility before all. I see two ways these design aspects may influence society. First, it may re-establish authentication as a security measure for the end-users and not a barrier. The participants other aspects of cool and fun can further engage users when using an authentication method. Both increased usability and UX makes it easier for the user to maintain security, ultimately increasing security for the users and organizations they are connected to. Making it easier for users to maintain security is increasingly important in the Information Society. Obviously for security reasons, but also because of the unexpected effects badly designed security can have in society. Some actors do not see how bad design or lack of security knowledge makes it difficult for users to maintain security. For example, as mentioned in Chapter 1, on the front page of Norwegian newspaper Dagens Næringsliv from May 8, 2015, lawyer Christian Sturla Svensen goes out and says he thinks employees should be fired for writing down passwords on notes [22]. A more usable user-authentication from an interaction design perspective can actually stabilize unexpected side-effects like this.

Secondly, the design aspects that emerged in this project can contribute to how to further accessibly design user-authentication. Given the important position user-authentication has for accessing the Information Society, contributing to a more universal user-authentication is important for digital participation. The Norwegian Government regards digital participation from all citizens crucial to ensure that ICT contributes to value creation and growth in society [52]. The Government is also honest on the fact that if you are not online, you will often feel excluded from society [52], but the requirements for how ICT is universally designed does not solve the first barrier vulnerable users often meet, which is a memory heavy user-authentication. An excluded person from the Internet will lose normalized ways of communicating within society. For long-term, teenage patients and other vulnerable users, better accessibly designed authentication methods will further ensure that they do not loose their sense of freedom and independence. But since all human beings have conceptual limits — for the future of society, passwords must be replaced by pass-gestures!

7.3 The Way Further

With regards to a final design of an authentication method, there are some big steps left. Of course the design process when following a use-oriented approach to PD is iterative and exploring, and the process would have been followed to its ‘end’. To be more concrete, there are some open questions that would have to be addressed. Though the user credential with the authentication factor(s) is the big core, an authentication method is more than the user credential. Chapter 5 Prototype: Pass-Gestures presents some unlisted open questions with regards to what would probably be next steps in the design process, which are summarized here. First, the design needs an intuitive user interface that supplements the hand gesture user credential. Providing a good, simple mental model is key here, but the interface must also support the cool and fun aspects of the design. In regards to the chose gesture being easy recallable, the interface may have to provide some visual clues to what gesture that is recorded during the enrollment stage. Next, further understanding the technical possibilities and limitations of hand gesture behavior is needed, e.g., is there a need for the user to identify beforehand.

The biggest challenge is how to actually replace passwords. The social group of those that develop web-based ICT must be persuaded to replace passwords, possibly by a domino effect started by Norway's change of its requirements for Universal Design of ICT.

Bibliography

[1] *"123456" Maintains the Top Spot on SplashData's Annual "Worst Passwords" List*. Jan. 20, 2015. URL: http://splashdata.com/press/worst-passwords-of-2014.htm (visited on 03/16/2015) (cit. on p. 10).

[2] Agency for Public Management and eGovernment (Difi). *Regulations on the universal design of ICT | Universell utforming - Difi*. Apr. 30, 2014. URL: http://uu.difi.no/english/ (visited on 05/08/2014) (cit. on pp. 5, 6, 14).

[3] *Ali Baba*. In: *Wikipedia, the free encyclopedia*. Page Version ID: 658119544. Apr. 22, 2015 (cit. on p. 2).

[4] Md Tanvir Islam Aumi and Sven Kratz. "AirAuth: Evaluating In-air Hand Gestures for Authentication." In: *Proceedings of the 16th International Conference on Human-computer Interaction with Mobile Devices & Services*. MobileHCI '14. New York, NY, USA: ACM, 2014, pp. 309–318 (cit. on pp. 45, 51, 70, 72, 73).

[5] E. Bardram. "The Trouble with Login: On Usability and Computer Security in Ubiquitous Computing." In: *Personal Ubiquitous Comput.* 9.6 (Nov. 2005), pp. 357–367 (cit. on p. 46).

[6] Nancy K. Baym. *Personal connections in the digital age*. Polity, 2010 (cit. on pp. 2, 3).

[7] David Benyon. *Designing Interactive Systems: A Comprehensive Guide to HCI and Interaction Design*. 2nd ed. Addison Wesley, 2010. 678 pp. (cit. on pp. 4–6, 38–40, 42, 43, 52, 67, 72, 82).

[8] Robert Biddle et al. "Graphical Passwords: Learning from the First Twelve Years." In: *ACM Comput. Surv.* 44.4 (Sept. 2012), 19:1–19:41 (cit. on pp. 52, 72, 73).

[9] Joseph Bonneau. "Guessing human-chosen secrets." Thesis. University of Cambridge, June 12, 2012 (cit. on p. 49).

[10] Reinhardt A. Botha et al. "From desktop to mobile: Examining the security experience." In: *Computers & Security* 28.3 (May 2009), pp. 130–137 (cit. on p. 43).

[11] Eva Brandt et al. "Tools and techniques: ways to engage telling, making and enacting." In: *Routledge International Handbook of Participatory Design*. Routledge International Handbooks. New York: Routledge, 2013, pp. 145–181 (cit. on pp. 20–22, 24, 27, 31).

[12] Tone Bratteteig et al. "Method: organising principles and general guidelines for Participatory Design projects." In: *Routledge International Handbook of Participatory Design*. Routledge International Handbooks. New York: Routledge, 2013, pp. 117–144 (cit. on pp. 18–20, 24).

[13] Marion Buchenau and Jane Fulton Suri. "Experience Prototyping." In: *Proceedings of the 3rd Conference on Designing Interactive Systems: Processes, Practices, Methods, and Techniques*. DIS '00. New York, NY, USA: ACM, 2000, pp. 424–433 (cit. on pp. 22, 57).

[14] Matthias Budde et al. "A Comparative Study to Evaluate the Usability of Context-Based Wi-Fi Access Mechanisms." In: *Universal Access in Human-Computer Interaction. Aging and Assistive Environments*. Ed. by Constantine Stephanidis and Margherita Antona. Lecture Notes in Computer Science 8515. Springer International Publishing, June 22, 2014, pp. 451–462 (cit. on p. 44).

[15] *Buypass Smartkort - Buypass.no*. URL: `http://www.buypass.no/bruker/buypass-id/buypass-smartkort` (visited on 03/30/2015) (cit. on p. 9).

[16] Andrew Clement et al. "Probing, mocking and prototyping: participatory approaches to identity infrastructuring." In: ACM Press, 2012, p. 21 (cit. on pp. 15, 16).

[17] Juli Clover. *Iris Scanning: The Newest Addition to Apple's Biometric Roadmap?* Jan. 21, 2014. URL: `http://www.macrumors.com/2014/01/21/apple-iris-scanning/` (visited on 02/02/2015) (cit. on p. 49).

[18] Shiran Cohen et al. "Towards Information Technology Security for Universal Access." In: *Universal Access in Human-Computer Interaction. Design for All and eInclusion*. Ed. by Constantine Stephanidis. Lecture Notes in Computer Science 6765. Springer Berlin Heidelberg, 2011, pp. 443–451 (cit. on p. 44).

[19] Alma Leora Culén and Andrea Alessandro Gasparini. "Situated Techno-Cools: factors that contribute to making technology cool in a given context of use." In: *PsychNology Journal* 10.2 (2012), pp. 117–139 (cit. on p. 41).

[20] Hua Dong. "Shifting paradigms in universal design." In: *Universal Acess in Human Computer Interaction. Coping with Diversity*. Springer, 2007, pp. 66–74 (cit. on pp. 5, 14).

[21] Stephen W. Draper. "Analysing fun as a candidate software requirement." In: *Personal Technologies* 3.3 (1999), pp. 117–122 (cit. on pp. 43, 79).

[22] Magnus Eidem. "Vil sparke folk etter dataslurv." In: *Dagens Næringsliv* (May 8, 2015), p. 5 (cit. on pp. 11, 79, 84).

[23] Fornyings-, administrasjons- og kirkedepartementet. *På nett med innbyggerne*. Regjeringen.no. Sept. 5, 2012. URL: `http://www.regjeringen.no/nb/dokumenter/pa-nett-med-innbyggerne/id698435/` (visited on 04/01/2015) (cit. on p. 2).

[24] Christopher Frayling. *Research in art and design*. Royal College of Art London, 1993, p. 7 (cit. on pp. 82, 83).

[25] *Fun*. In: *Wikipedia, the free encyclopedia*. Page Version ID: 661938384. May 12, 2015 (cit. on p. 42).

[26] Dan Goodin. *Why passwords have never been weaker—and crackers have never been stronger*. Ars Technica. Aug. 21, 2012. URL: `http://arstechnica.com/security/2012/08/passwords-under-assault/` (visited on 03/18/2014) (cit. on p. 1).

[27] *Hacker (computer security)*. In: *Wikipedia, the free encyclopedia*. Page Version ID: 657126582. Apr. 19, 2015 (cit. on p. 10).

[28] Marc Hassenzahl and Noam Tractinsky. "User experience - a research agenda." In: *Behaviour & Information Technology* 25.2 (Mar. 1, 2006), pp. 91–97 (cit. on pp. 39, 40, 43, 54).

[29] Cormac Herley et al. "Passwords: If We're So Smart, Why Are We Still Using Them?" In: *Financial Cryptography and Data Security*. Ed. by Roger Dingledine and Philippe Golle. Lecture Notes in Computer Science 5628. Springer Berlin Heidelberg, Jan. 1, 2009, pp. 230–237 (cit. on p. 13).

[30] Sean Hollister. *Could the NSA use Microsoft's Xbox One to spy on you?* The Verge. July 16, 2013. URL: `http://www.theverge.com/2013/7/16/4526770/will-the-nsa-use-the-xbox-one-to-spy-on-your-family` (visited on 04/21/2015) (cit. on p. 44).

[31] Karen Holtzblatt. "What Makes Things Cool?: Intentional Design for Innovation." In: *interactions* 18.6 (Nov. 2011), pp. 40–47 (cit. on p. 43).

[32] Matthew Horton et al. "Too Cool at School-Understanding Cool Teenagers." In: *PsychNology Journal* 10.2 (2012), pp. 73–91 (cit. on p. 41).

[33] A.K. Jain et al. "Biometrics: A Tool for Information Security." In: *IEEE Transactions on Information Forensics and Security* 1.2 (June 2006), pp. 125–143 (cit. on pp. 9, 37, 47, 49–51).

[34] Patrick W. Jordan. "Human factors for pleasure in product use." In: *Applied Ergonomics* 29.1 (Feb. 1998), pp. 25–33 (cit. on pp. 39, 53).

[35] Audun Jøsang et al. "Usability and Privacy in Identity Management Architectures." In: *Proceedings of the Fifth Australasian Symposium on ACSW Frontiers - Volume 68*. ACSW '07. Darlinghurst, Australia, Australia: Australian Computer Society, Inc., 2007, pp. 143–152 (cit. on pp. 13, 45).

[36] Erik Kain. *NSA Domestic Spying Program Makes Xbox One Even Scarier*. Forbes. June 7, 2013. URL: `http://www.forbes.com/sites/erikkain/2013/06/07/nsa-domestic-spying-program-makes-xbox-one-even-scarier/` (visited on 04/21/2015) (cit. on p. 44).

[37] Michael Karlesky et al. "Open Sesame: Re-envisioning the Design of a Gesture-based Access Control System." In: *CHI '13 Extended Abstracts on Human Factors in Computing Systems*. CHI EA '13. New York, NY, USA: ACM, 2013, pp. 1167–1172 (cit. on p. 44).

[38] Finn Kensing and Joan Greenbaum. "Heritage: having a say." In: *Routledge International Handbook of Participatory Design*. Routledge International Handbooks. New York: Routledge, 2013, pp. 21–36 (cit. on pp. 13, 17, 18, 21).

[39] Adrian Kingsley-Hughes. *The iPhone 5s fingerprint reader: More about convenience than security*. ZDNet. Oct. 8, 2013. URL: http://www.zdnet.com/article/the-iphone-5s-fingerprint-reader-more-about-convenience-than-security/ (visited on 01/30/2015) (cit. on pp. 10, 50).

[40] Sarah Knapton. *Why your fingerprints may not be unique*. Apr. 21, 2014. URL: http://www.telegraph.co.uk/news/science/science-news/10775477/Why-your-fingerprints-may-not-be-unique.html (visited on 01/23/2015) (cit. on p. 9).

[41] Ravi Kuber and Shiva Sharma. "Toward Tactile Authentication for Blind Users." In: *Proceedings of the 12th International ACM SIGACCESS Conference on Computers and Accessibility*. ASSETS '10. New York, NY, USA: ACM, 2010, pp. 289–290 (cit. on p. 43).

[42] *KULU - Cool technologies for youth with long-term health challenges*. URL: http://kulu.no/?lang=en (visited on 05/03/2015) (cit. on p. 13).

[43] *Leap Motion*. URL: https://www.leapmotion.com/product (visited on 05/03/2015) (cit. on pp. 22, 23, 69).

[44] Jonas Löwgren and Erik Stolterman. *Thoughtful interaction design: A design perspective on information technology*. Mit Press, 2004 (cit. on pp. 19, 20, 67, 68, 83).

[45] L. Lynch. "Inside the Identity Management Game." In: *IEEE Internet Computing* 15.5 (Sept. 2011), pp. 78–82 (cit. on p. 43).

[46] Yao Ma et al. "Investigating User Behavior for Authentication Methods: A Comparison Between Individuals with Down Syndrome and Neurotypical Users." In: *ACM Trans. Access. Comput.* 4.4 (July 2013), 15:1–15:27 (cit. on pp. 7, 8, 47).

[47] Margaret Machniak. "In pursuit of cool and its implications for the design process." In: *Culture, Technology, Communication* (2014), p. 66 (cit. on pp. 41, 66).

[48] Raymond Madden. *Being ethnographic: A guide to the theory and practice of ethnography*. Sage Publications, 2010 (cit. on pp. 27, 68).

[49] Stephen M. Matyas Jr. and Jeff Stapleton. "A Biometric Standard for Information Management and Security." In: *Computers & Security* 19.5 (July 1, 2000), pp. 428–441 (cit. on pp. 7, 47).

[50] John F. McGowan. *Are Fingerprints Unique?* Sept. 20, 2011. URL: http://math-blog.com/2011/09/20/are-fingerprints-unique/ (visited on 01/15/2015) (cit. on p. 9).

[51] Ministry of Local Government and Modernisation. *Report No. 17 (2006 - 2007) to the Storting: An Information Society for All*. 071001-040005. Jan. 16, 2007. URL: http://www.regjeringen.no/en/dokumenter/report-no-17-2006---2007-to-the-storting/id441497/ (visited on 04/11/2015) (cit. on pp. 3–5, 14).

[52] Ministry of Local Government and Modernisation. *Digital Agenda for Norway — Meld. St. 23 (2012-2013) Report to the Storting (white paper)*. Government.no. Nov. 16, 2014. URL: http://www.regjeringen.no/en/dokumenter/meld.-st.-23-2012-2013/id718084/ (visited on 04/02/2015) (cit. on pp. 2, 3, 84).

[53] R. Moskovitch et al. "Identity theft, computers and behavioral biometrics." In: *IEEE International Conference on Intelligence and Security Informatics, 2009. ISI '09*. IEEE International Conference on Intelligence and Security Informatics, 2009. ISI '09. June 2009, pp. 155–160 (cit. on p. 35).

[54] Donald A. Norman. *The design of everyday things*. Basic books, 2002 (cit. on pp. 9, 72).

[55] Donald A. Norman. "THE WAY I SEE IT: When Security Gets in the Way." In: *interactions* 16.6 (2009), pp. 60–63 (cit. on pp. 10, 35, 79).

[56] L. O'Gorman. "Comparing passwords, tokens, and biometrics for user authentication." In: *Proceedings of the IEEE* 91.12 (Dec. 2003), pp. 2021–2040 (cit. on pp. 1, 7, 8, 13, 35, 47, 51, 53).

[57] "Personal authentication using heart sound waveform and/or breathing waveform pattern." 20060293606. Seijiro Tomita. Dec. 28, 2006 (cit. on p. 47).

[58] Melanie Pinola. *Why you need a password manager (besides saving your passwords)*. ITworld. Apr. 14, 2015. URL: http://www.itworld.com/article/2909645/why-you-need-a-password-manager-besides-saving-your-passwords.html (visited on 04/23/2015) (cit. on p. 9).

[59] Laura Poitras. *Citizenfour*. In collab. with Edward Snowden et al. Feb. 23, 2015 (cit. on p. 50).

[60] Anabel Quan-Haase. *Technology and Society: Social Networks, Power, and Inequality*. 1st ed. Oxford University Press, 2013 (cit. on pp. 3, 11, 12, 75, 77).

[61] Martin Rasmussen and Floyd Webster Rudmin. "The Coming PIN Code Epidemic: A First Study of Memory of Numeric Security Codes." In: *E-Journal of Applied Psychology* 6.2 (Dec. 30, 2010) (cit. on p. 9).

[62] Janet C. Read et al. "On being cool: exploring interaction design for teenagers." In: *Proceedings of the 27th International BCS Human Computer Interaction Conference*. British Computer Society, 2013, p. 10 (cit. on pp. 41, 42, 54, 66).

[63] Janet Read et al. "Understanding and Designing Cool Technologies for Teenagers." In: *CHI '11 Extended Abstracts on Human Factors in Computing Systems*. CHI EA '11. New York, NY, USA: ACM, 2011, pp. 1567–1572 (cit. on p. 54).

[64] Chris Riley et al. "Instruction, Feedback and Biometrics: The User Interface for Fingerprint Authentication Systems." In: *Human-Computer Interaction – INTERACT 2009*. Ed. by Tom Gross et al. Lecture Notes in Computer Science 5727. Springer Berlin Heidelberg, 2009, pp. 293–305 (cit. on p. 15).

[65] Toni Robertson and Jesper Simonsen. "Participatory Design: an introduction." In: *Routledge International Handbook of Participatory Design*. Routledge International Handbooks. New York: Routledge, 2013, pp. 1–18 (cit. on pp. 17, 18).

[66] Elizabeth B.-N. Sanders and Pieter Jan Stappers. "Co-creation and the new landscapes of design." In: *CoDesign* 4.1 (Mar. 1, 2008), pp. 5–18 (cit. on pp. 17–21).

[67] M. A. Sasse and I. Flechais. "Usable Security: Why Do We Need It? How Do We Get It?" In: *Security and Usability: Designing secure systems that people can use*. Ed. by L. F. Cranor and S. Garfinkel. Sebastopol, US: O'Reilly, 2005, pp. 13–30 (cit. on pp. 35, 49, 79, 83).

[68] Mahadev Satyanarayanan. "Pervasive computing: Vision and challenges." In: *Personal Communications, IEEE* 8.4 (2001), pp. 10–17 (cit. on p. 3).

[69] Bruce Schneier. *Biometrics: Truths and Fictions*. 1998. URL: `https://www.schneier.com/crypto-gram/archives/1998/0815.html#biometrics` (visited on 01/28/2015) (cit. on pp. 51, 53).

[70] *Security Now 440*. TWiT.tv. Jan. 28, 2014. URL: http://www.twit.tv/show/security-now/440 (visited on 04/13/2015) (cit. on p. 10).

[71] Ben Shneiderman. "Designing for Fun: How Can We Design User Interfaces to Be More Fun?" In: *interactions* 11.5 (Sept. 2004), pp. 48–50 (cit. on p. 43).

[72] Dobromir Todorov. *Mechanics of user identification and authentication: Fundamentals of identity management*. CRC Press, 2007 (cit. on pp. 6, 7, 47, 49, 53, 63, 69).

[73] *Touch ID not working for you? Here's a fix!* iMore. URL: http://www.imore.com/touch-id-not-working-you-heres-fix (visited on 04/13/2015) (cit. on p. 10).

[74] *Unlock your Phone Differently with Picture Password LockScreen – App Review*. In collab. with xdadevelopers. Nov. 1, 2012 (cit. on p. 52).

[75] William Usher. *Is the Xbox One a Covert Surveillance Device?* Infosecurity Magazine. May 28, 2013. URL: http://www.infosecurity-magazine.com/news/is-the-xbox-one-a-covert-surveillance-device/ (visited on 04/21/2015) (cit. on p. 44).

[76] Maja van der Velden and Christina Mörtberg. "Participatory Design and Design for Values." In: *Handbook of Ethics, Values, and Technological Design*. Ed. by Jeroen van den Hoven et al. Springer Netherlands, 2014, pp. 1–22 (cit. on pp. 17, 75, 76).

[77] Peter-Paul Verbeek. "Morality in Design: Design Ethics and the Morality of Technological Artifacts." In: *Philosophy and Design*. Springer Netherlands, Jan. 1, 2008, pp. 91–103 (cit. on pp. 11, 12, 75, 78).

[78] Rene Victor Valqui Vidal. *The Future Workshop: Democratic Problem Solving*. Informatics and Mathematical Modelling, Technical University of Denmark, DTU, 2005 (cit. on pp. 21, 22, 29, 31, 32, 46).

[79] Kim-Phuong L. Vu et al. "Improving password security and memorability to protect personal and organizational information." In: *International Journal of Human-Computer Studies* 65.8 (Aug. 2007), pp. 744–757 (cit. on pp. 8, 10).

[80] *Web 2.0*. In: *Wikipedia, the free encyclopedia*. Page Version ID: 662166137. May 13, 2015 (cit. on p. 3).

[81] Mark Weiser. “The Computer for the 21st Century.” In: *Scientific American* 265.3 (Sept. 1991), pp. 94–104 (cit. on pp. 3, 6, 10).

[82] *Why I hacked TouchID (again) and still think it’s awesome | Lookout Blog*. URL: `https://blog.lookout.com/blog/2014/09/23/iphone-6-touchid-hack/` (visited on 04/13/2015) (cit. on p. 9).

[83] *Xbox One Kinect Is A Surveillance Device, Says Australia’s Civil Liberty Director | CINEMABLEND*. URL: `http://www.cinemablend.com/games/-Xbox-One-Kinect-Surveillance-Device-Says-Australia-Civil-Liberty-Director-56126.html` (visited on 04/21/2015) (cit. on p. 44).

Appendices

Appendix A

Preparations for Workshop I: Future Workshop

A.1 Plan of What to Say

Hei jeg heter Johan og jeg har gjort klar en liten workshop som består av tre forskjellige deler eller faser. Og i hver forskjellig fase skal vi skrive ideer på post-it-lapper, og den sin idé det var skriver sitt ID nr på lappen.

A.1.1 (Passord) kritikk — Kritikk fasen (5 min)

Tykke tusjer + post-it (rød) for å skrive ned meningene å klistre på tavle/papirrull.

Vi skal starte med å snakke om hvordan dere logger inn på en online tjeneste, feks facebook, google, banken og andre ting, både på PC-en, mobilen, tablet, andre ting.

- Så hvilke forskjellige metoder bruker dere til å logge inn? Er det passord, PIN-kode, andre ting, osv.
- La oss starte med passord. Hva synes dere om passord? Har dere noe kritikk til passord? Kan alle bruke passord?
- Hva synes vi om de andre måtene å logge inn på?
- Hvor mange forskjellige passord har du?
- Hvor ofte bytter du passord?

- Hvordan lager du passord?
- Hvordan er det å huske passord?
- Er det noen andre problemer dere tror andre folk kan ha?

A.1.2 Din drømme innlogging — Fantasi fasen (10 min)

Tykke tusjer + post-it (grønn) for å skrive ned meningene så klistre på tavle/papirrull.

I denne fasen skal vi ikke tenk på hva som faktisk går ann. Nå er det bare helt fri brainstorming. Her går det bra med rare, morsomme, sprø, ulogiske ideer.

- Har dere noen ideer til hvordan man kunne ha logget inn?
- Hvis dere skulle tenke dere den enkleste/morsomste måten å logge inn på, hva ville det ha vært?
- Eller bare andre måter å logge inn på?
- Din drømme innlogging, hvordan hadde den vært?

Sist i fasen: Sotere post-it basert på kult, flytte over til kult på tavla/papirrullen. Ikke stemme ned ('ukult'):

- Hva liker dere best? Hva er det som gjør at du syns det?

A.1.3 Realisme/Meninger — Realisme fasen (5 min)

Tykke tusjer + post-it (blå) for å skrive ned meningene så klistre på tavle/papirrull.

Av de ideene vi har:

- Er (de best likte) ideene brukbar for alle (universell utforming)? Hva kan gjøres med det?

Appendix B

Preparations for Workshop II: Experience Prototyping

B.1 Use-Oriented Design Cycle (see fig. 2.1) Progress

Real life problem situation is described in Chapter 1 Introduction.

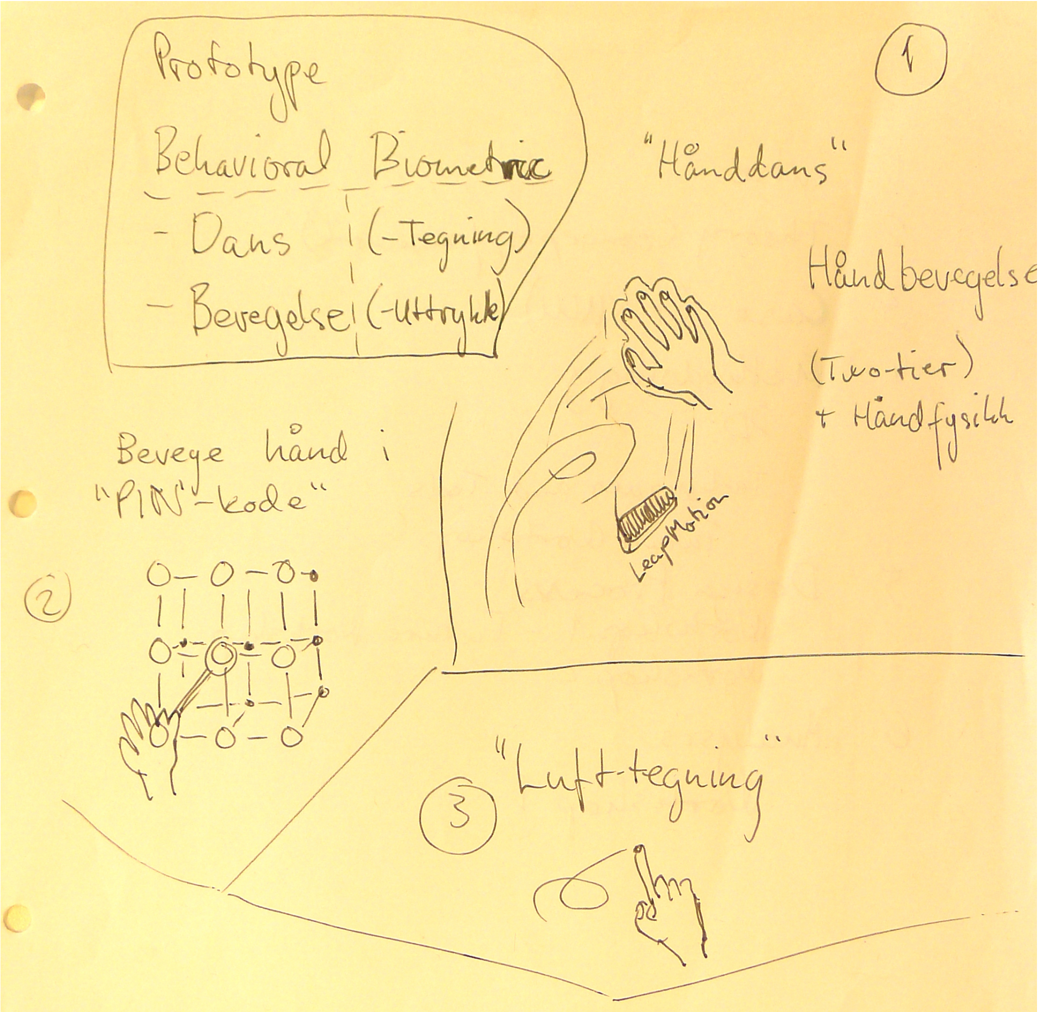
Understanding practice. How do teenage patients use authentication. What do they choose to use and do? Answers from workshop 1, critique phase: Facebook's login, sharing passwords, using same passwords, struggling remembering passwords. They work around security to ease the use of authentication/login — comfort before security — even when they know security is compromised (which is a general user reaction in relation to security). What are the practices within authentication design?: Analysis, with literature review, of workshop 1.

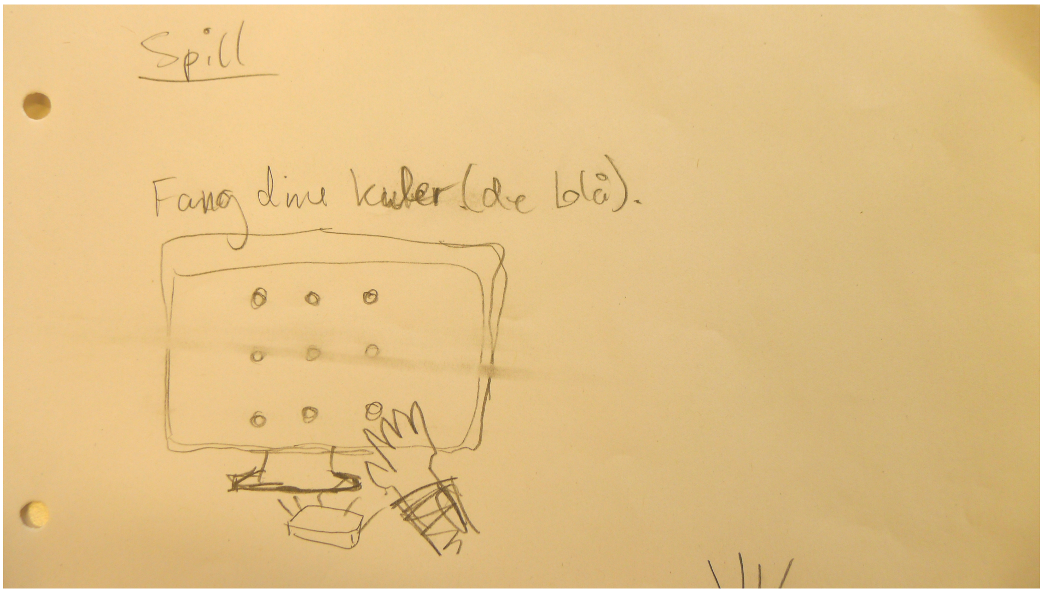
Identifying needs, wishes Workshop 1 did not explicitly identify needs and wishes, but from an interpretation of the suggestions, results may imply the need/wish for: simplicity of use (face and voice recognition, biometric recognition of sorts, ID tag); fun use (dance, movement, drawing, game, voice), or; 'cool/hip' (voice, taking a selfie, game, dance, drawing, iris scanning); there were also comical aspects (telling a dirty joke, logging in with your tongue).

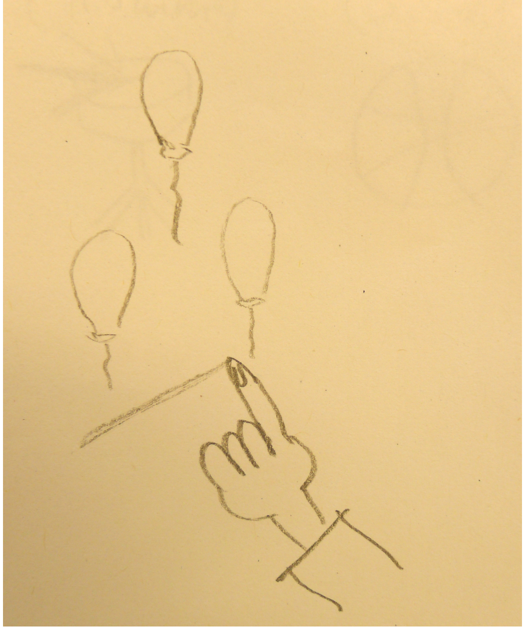
Describing requirements (Preparing suggestions further — based on literature)

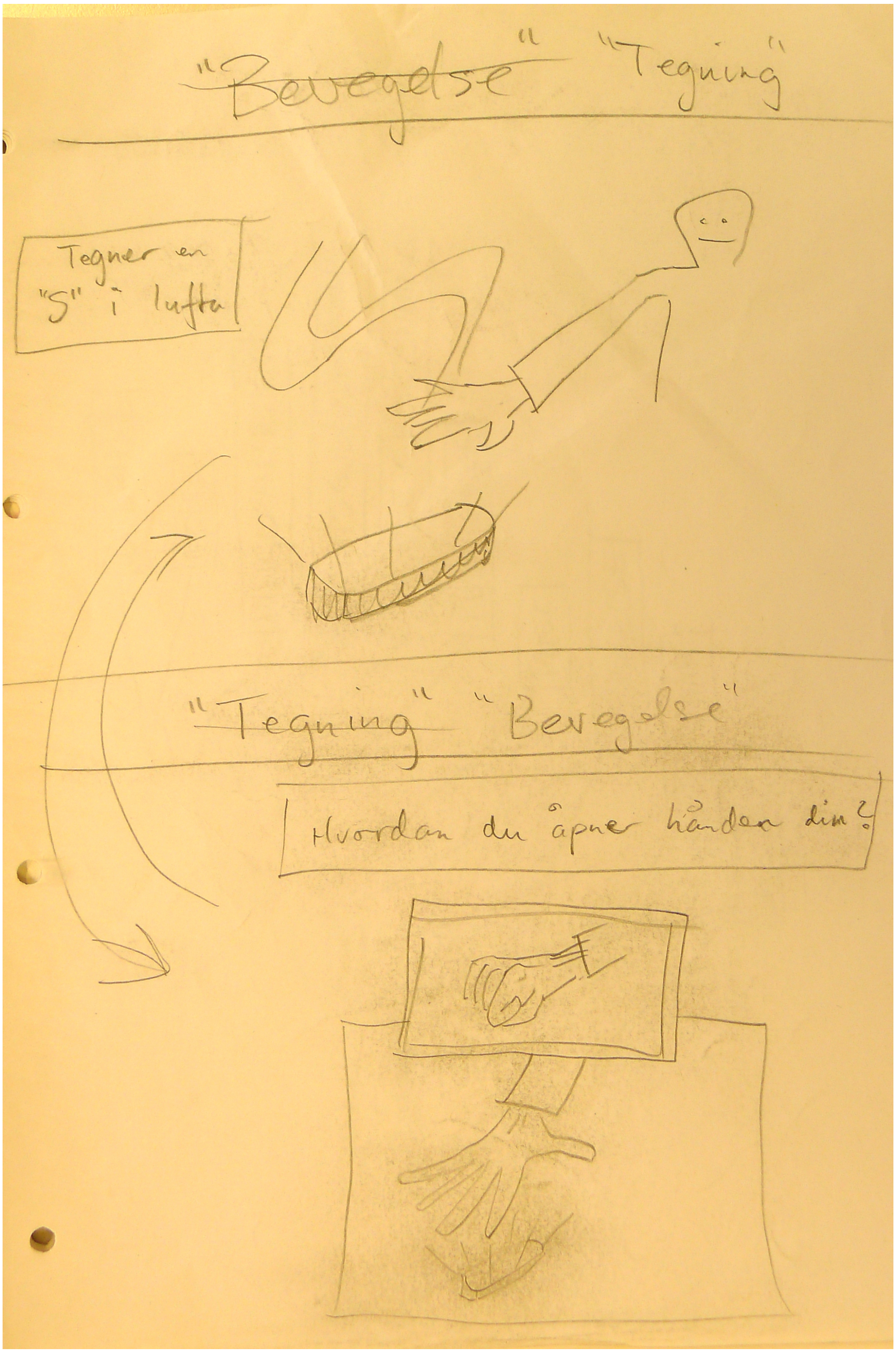
Concretizing, materializing (In preparation for, and during workshop 2, and after)

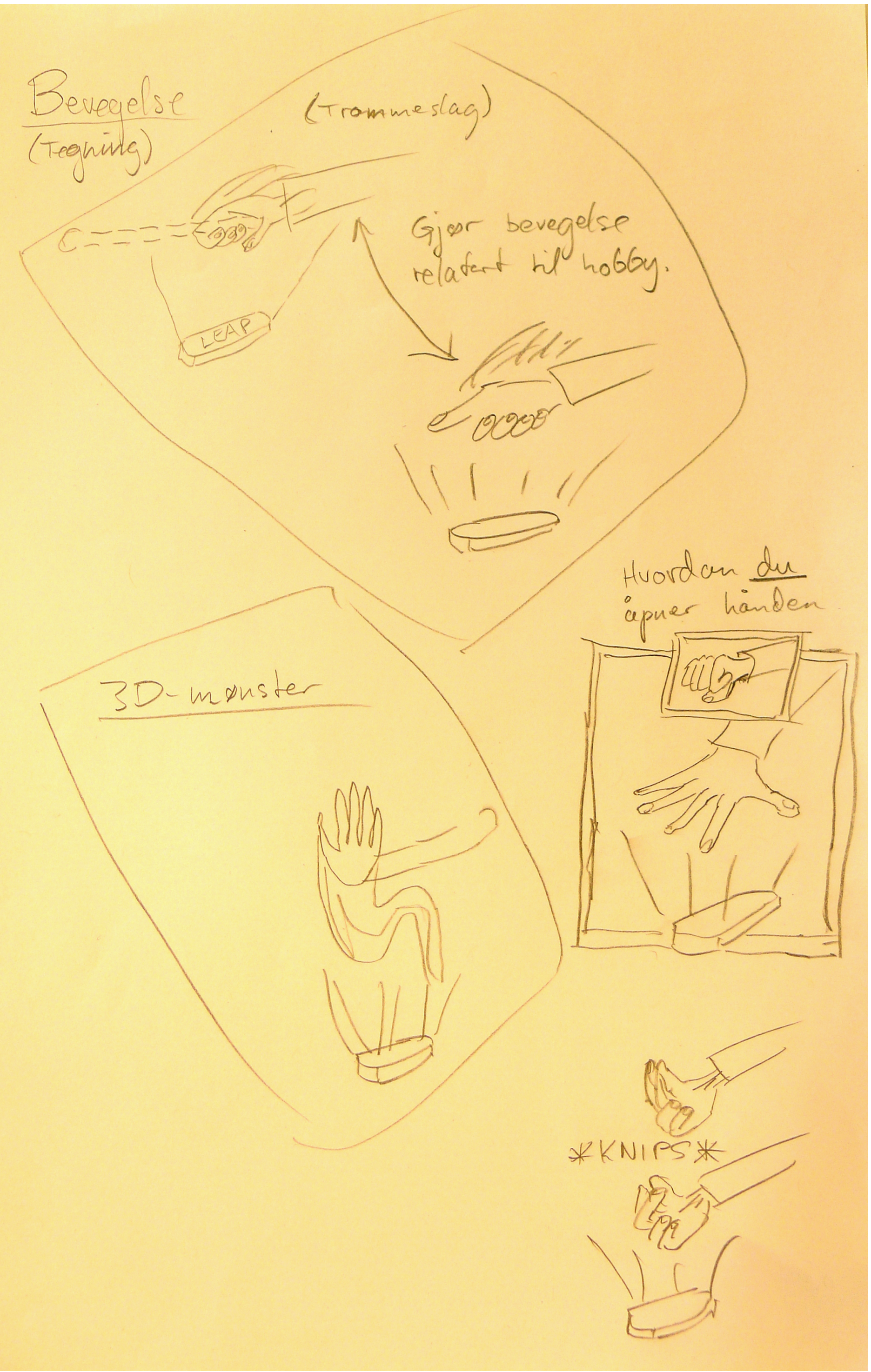
B.2 Sketches




Spill
Fang dine kuler (de blå).




~~"Bevegelse"~~ "Tegning"
Tegner en "S" i lufta
~~"Tegning"~~ "Bevegelse"
Hvordan du åpner hånden din?


Bevegelse
(Tegning)
(Trommeslag)
LEAP
Gjør bevegelse relatert til hobby.
Hvordan du åpner hånden
3D-mønster
KNIPS

B.3 Survey

(Next page)

3 kjappe spørsmål | Ditt ID-nr.: _____

1. Hadde du likt å logge inn på PCen ved hjelp av LeapMotion (eller det å bruke bevegelse)? Kryss av i én rute [X]

1 - likt veldig lite	2 - likt lite	3 - likt nøytralt	4 - likt godt	5 - likt veldig godt

2. Og hvorfor? Er det morro/ikke-morro, kult/ikke-kult, og lettvint/slitsomt, eller noe annet?

3. Hvordan ville du likt å logge inn på PCen ved hjelp av eksemplene under? Kryss av [X]

	Veldig lite	Lite	Nøytralt	Likt godt	Likt veldig godt	Eventuelt skriv hvorfor (f.eks. morro/ikke-morro, kult/ikke-kult, og lettvint/slitsomt)
Egangskode til mobil						
Finger-avtrykk						
Ansikts-gjenkjenning						

4. Kommentar?