Two Key PIN Entry Method for Public Access Terminals: Evaluated with a Method Using Principles from Universal Design and Safety.

Einar Krokan

Master's Thesis
Master of Science in Information Security
30 ECTS
Department of Computer Science and Media Technology
Gjøvik University College, 2012

Avdeling for
informatikk og medieteknikk
Høgskolen i Gjøvik
Postboks 191
2802 Gjøvik

Department of Computer Science
and Media Technology
Gjøvik University College
Box 191
N-2802 Gjøvik
Norway

Abstract

This thesis takes a look at universal design and it's principles to test a new personal identity number (PIN) entry method with public access terminals. We argue that universal design can not only make the evaluated solution better for more people, but may also solve other problems. A new model combining ideas from universal design, security and safety where the user interface is looked at as a set of modalities sending messages back and forth between the user and the system is used to evaluate the human computer interaction of the PIN entry method. Instead of looking at how users disabilities restricts their usage of the system we look at it as another constriction to the usage. Constriction do not apply only to the user, but also to the device, environment and social settings. The same messages can be intercepted by a third party to gain unauthorized insight of the information. The evaluation method was used on a novel prototype payment terminal and was tested on a group of users with visual constrictions and a group with normal vision to see if the new PIN entry method was usable and more secure. The PIN entry method was found easy to learn and use by both groups, but was slower and only showed a little improvement against observation attacks. The evaluation method was useful to get a good understanding on how different effects from modalities is restricted by different factors and that the same effects could influence the possibility for observation attack. We further think that by divide possible errors into intentional and unintentional and difference between violations and normal errors is helpful for designing system where people are involved. The need to create simple and standard user interfaces, remove unnecessary elements that is not needed for the user, are something that should improve both accessibility and security for everyone using payment terminals.

Acknowledgements

I want to thank my supervisor Kirsi Helkala for valuable input, discussion and help during the writing of this thesis. I would also like to thank all participants of the experiment for taking the time to test our new PIN entry method and providing us with valuable input during the interviews. Last but not least I want to thank my two kids Anine and Mats for being patient when their father when he spent to much time in front of the computer the last months writing this thesis instead of spending time with them.

Einar Krokan, 30th June 2012

Contents

1 Introduction

1.1 Topic covered

Public access terminals like ATMs and payment terminals is something people use almost daily. Most of us are familiar with the procedure to use them and find it easy and mostly a routine. The authentication procedure is handled by identifying us with the help of a plastic card equipped with a magnetic stripe or an electronic chip against the terminal. A four digit personal identification number (PIN code) is the secret that we provide to the terminal to prove we are the rightful owner of the card.

Universal design is a way of thinking when designing solutions that should be available for everyone regardless of disabilities. This design philosophy should be used when designing public access terminals as well to make both the usability and accessibility better for everyone. Universal design is not always used from the start of a design process and improvements for people with different disabilities are added after the first version of the solution is finished. Because you have to think a bit different and creatively when finding solutions that will work for people with disabilities we hope that by using these principles we can come up with solutions that are both more accessible and more secure for everyone. Fuglerud et al.[22] pointed out that the lack of standardization for such terminals could be a challenge for everyone, but an even bigger problem for certain groups.

Safety planning has some similarities with security and applying that when designing authentication solutions could help us identify more security weaknesses and why people end up doing errors that can lead to security incidents.

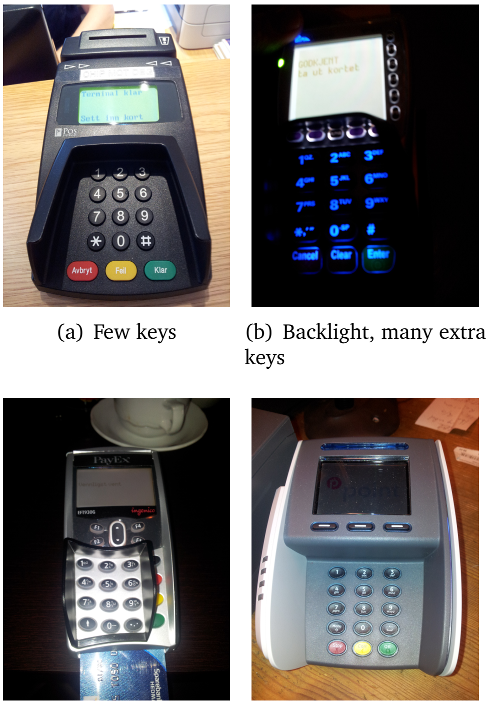
In this thesis we will take a look at a model that could help when evaluating authentication solutions and that take universal design into consideration from the beginning. The model is used on a new method for entering the PIN code that came from our wish to create a better solution for people with visual impairments. We use our model and principles from universal design to evaluate it and hope we can present a simpler and more secure PIN entry method for everyone. Our idea is that by thinking creatively to solve a unique problem for a group with special needs we can come up with solutions that is both better for everyone and at the same time be more secure against some types of security vulnerabilities.

1.2 Keywords

Universal design, Security, Authentication, Public Access Terminals, ATM, PIN, Visual disabilities, Shoulder surfing

1.3 Problem description

ATM and payment terminal functionality is rather limited and should be simple to use for everyone. Different vendors create these terminals with different user interfaces that make it more difficult than necessary. The card can be inserted at different places on the terminal, sometimes in front, sometimes on the top and even on the sides. If the chip should be facing you or not is not clear and extra written signs are sometimes provided to help. For normal use we only use the 0-9 keys together with the enter key and sometimes the cancel button if you make a mistake. Terminal vendors places the keys at different locations and in different order. Some terminals have many extra keys that is not in use or not for normal operations. For people that have visual or cognitive disabilities this can be challenging and the need to create simpler and more standard solutions is important.



(a) Few keys (b) Backlight, many extra keys

(c) Control keys on right side (d) New termial with NFC reader.

Figure 1: Examples of payment terminals with different design.

From media we read and see that people get their credit cards pickpocket and at the same time the PIN code lost by criminal's observing the pin entry when you use it through the use of cameras, binoculars, mirrors or just shoulder surfing you when standing in line at the terminals [13]. This is often sufficient for the criminals to emptying your accounts before you notice the card is stolen. According to Finansnæringens Fellesorganisasjon in Norway [13] this type of crime is responsible for almost 20% of the banks losses when it comes to payment and credit cards. For people with disabilities like blindness it can be even harder to see if they are observed or the terminal they use is tampered with.

The increasing use of public terminals and the need for more knowledge of challenges for different user groups with the use of authentication solutions when it comes to usability, accessibility, security and privacy is needed.

1.4 Justification motivation and benefits

From media we get reminded quite often about different kinds of scams and crimes that happens in connection with ATMs, credit cards, PIN codes and payment terminals [3] [19] [28] [28]. Skimming equipment placed on ATMs made to steal both cards, money and PIN codes. Criminal's pickpocketing people for their credit cards and by looking over their shoulder retrieve the PIN code. In just a few minutes they empty or withdraw large amount from peoples accounts before they notice the card is missing and is able to call your bank to lock it. Banks and credit card companies create guidelines on how people should make sure no one watches as they type the pin by covering the hand entering the numbers on the key pad. The guidelines is often not followed. A Dutch report [9] found that 45% of people they observed using ATMs did not cover the PIN entry because of different distractions. The same guidelines also states that the PIN code should not be written down and credit card given away to other persons. If the card is misused because guidelines is not followed the bank may not cover the financial loss. On the other hand blind people have difficulties [16] [17] from a usability perspective where many end up breaking these rules by giving away their PIN code to strangers because the usability is not good enough. We may instead of blaming the users start thinking about maybe the ATMs and payment terminals have a usability problem and that we should start looking for new ways of solving the problems by changing the solution instead of pointing at the users. The idea is that by designing solutions from the start with universal design in mind we might come up with solutions that may not only benefit users with disabilities, but also solve security challenges for everyone.

1.5 Research questions

1.5.1 Question 1

How could we design a authentication system that uses principles from universal design and at the same time solve security challenges for everyone?

Our approach to this is to expand a model [32] where a users disability is not thought of as a problem, but only an restriction to the interaction. The model can be used not only to see how the system works for different user groups, but also how the system can be designed so other people can use the system under sub optimal conditions. Observation attacks like shoulder surfing make use of the same interaction between the user and the system to gain unauthorized access and we think we can expand the model7.1 to also include security. We have an idea for a new simple way of entering PIN codes discussed in Section 7.1 that we think could have the potential for being easier to use for visual impaired users and at the same time is more resilient to observation attacks like shoulder surfing. We want to evaluate the new PIN entry method with the enhanced model shown in Section 5 to see if the model is useful for identifying both usability challenges for different kinds of constrictions and security risks. We would have to test our new PIN entry method both with visual impaired users and people with normal sight to see if the PIN entry method is both usable and more resilient against shoulder surfing.

1.5.2 Question 2

How does our PIN entry method compare too today's PIN entry method where numeric keys are used for people with visual impairments and people with normal sight?

We want to see if our PIN entry method is usable both for visual impaired people and at the same time is usable for everyone. If our evaluation model can identify this or if the model have shortcomings would have to be investigated. To compare the PIN entry methods we will have try to find out how the two input methods compare to tree different variables, usability, universal design and security.

Sub question 2.1: How does the two PIN entry methods compare when it comes to usability?

Usability can be defined in multiple ways. One definition given by ISO [1] is "The extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use." Another popular view is given by Nilsen [30] where he looks at usability as learnability, efficiency of use, memorability, few and non-catastrophic errors and subjective satisfaction. Bevan [5] compares these two definitions and says that Nilsen looks more on the usability of the product itself, but ISOs definition looks more on the usability of the entire system.

We have chosen to look closer at usability in the terms used by Nilsen [30]:

- Learnability : How easy is it to learn the PIN entry methods.
- Efficiency of use : How efficient is the method to use measured in time spent.
- Memorability : When learned how easy is the new input method to remember.
- Few and non-catastrophic errors : Is the method more resilient to doing errors.
- Subjective satisfaction : How is the user satisfaction with the methods.

Sub question 2.2: How does the two PIN entry methods compare when it comes to accessibility for visual impaired users?

With accessibility we mean how easy it is to approach and use the PIN entry method for visual impaired users. We will focus on this group of users as the idea for the PIN entry method came from a wish to make it simpler for them. We will use principles from universal design to further evaluate our solution and the old PIN entry method.

Sub question 2.3: How does the two PIN entry methods compare when it comes to security and in particular observation attacks where the goal is to retrieve the entered PIN code?

Security is a very broad term and in our case we will look at it from an information security perspective. Even that is a wide topic and we will only look at a specific security challenge and that is how easy/difficult it is for a third party to observe and learn the PIN by the typing of the PIN on the payment terminal. How security is handled inside the terminal, the challenge of remembering pin codes, the entropy of the 4 digit PIN-code and so on is not in the scope of this thesis.

1.6 Planned contribution

Our goal with this thesis is that our new model could be helpful for people designing authentication solution where universal design is taken into consideration from the beginning. To early discover usability issues and security problems would be beneficial both for the designers and the users of the system. We hope our new PIN entry method will be well received by the group of people with visual constrictions and that the solutions does not have worse usability than the old method. In addition to this we hope that the solution shows improvements in regard to observation attacks like shoulder surfing. We do not expect the solution to be something that can be used directly in real life solutions, but hope that we can show that by using ideas from universal design we can make differences in other areas like security.

2 Related work

In this chapter we will take a look at related work to the problem description. According to Fuglerud and Dale [16] and Saxena et al. [38] relatively little research on authentication, usability and universal design together has been done in the past. We will therefore look at the work done in the different sub areas related to the main problem description and see if we can find models or other information that can shed light on the problem.

2.1 Universal design

Different definition and terms is used to describe universal design. The term Universal Design was first used by Ron Mace who was the founder of The Center for Universal Design. Different terms is used in different literature and regions to describe the same. 'Design for all' is common in EU. 'Inclusive design' and 'Universal Access' is all terms that is used to describe this, but with slightly different meaning. Universal design, design for all and inclusive design are all trying to describe how we should design solutions for use in everyday life so that all people, regardless of disability, age, race, cognitive skill and so on can use them. Stephanidis [39] uses the term universal access as approaches to accessibility to computer based applications used by users with disabilities.

Fuglerud et al. [22] looked at the universal design of different authentication and registration solutions. They went trough many different authentication solutions and looked at them from a usability standpoint for people with blindness and dyslectic difficulties. They identified challenges and problems with common security mechanisms. The main goal of the report was to identify and describe different challenges, success factors and research needs in regards to universal design. The participants in there tests experience with ATMs and payment terminals was described and the following challenges was described. Different keyboard layouts, difference in operation sequences from terminal to terminal, the lighting condition and touch screens was mentioned as challenges. A project where Norwegian ATMs was enhanced with audio menus to help people with vision problems are mention as one solution to design for universal design. The report concludes that it can be difficult to find one single solution that will fit all kinds of constriction and that maybe the solutions have to support multiple different ways of solving the same problem. The ATM with audio menus is an example of this where it supported both the regular way with screen for seeing, but at the same time supporting sound for people who like that. On the other hand as we stated in the problem description the sound menu was just added as an enhancement to an already existing solution instead of designing it from the start with universal design in mind.

In an another article Fuglerud and Dale [16] mention different authentication solutions that has improved the usability for some groups, but on the other hand is not usable by others. For instance is an technique where the user instead of a normal password/pin has to remember an set of pictures. It is known to be easier to remember this than a normal password, but for people with vision disabilities this solution is difficult to use. An rough analysis of different authentication methods for different groups of people with disabilities was presented and none of them was usable for everyone.

In Stephanidis book [39] a chapter on design of public access terminal gives details on different guidelines and standards for designing public access terminals so they are more accessible and usable for people with disabilities. Different direction to how to approach the design like audio output, tactile indicators, how the physical buttons should be raised and distance between them, to labels, fonts and colours of both keys and the screen display are given. As Fuglerud et al [22] also Stephanidis [39] says that it may be difficult to find one solution that works for every group of people and they says that it would be best if the solution could adapt to the user. They conclude that even when most manufacturer of public access terminals have taken the diversity of humans interacting into consideration we still have a long way to go to before it is incorporated into real systems.

2.2 Security

Authentication solutions is vulnerable to different kinds of observation attacks. When authentication occurs the user have to provide a secret and present this to the system. If a third party is able to somehow see or observe what the user presents to the system the attacker can later use what he have gathered and use it to gain access. The observation can happens from within the system where malware is installed and is placed between the input device of the system and the application who performs the authentication. Examples of this is key loggers. The attacker can also manipulate the input device from the outside so the user thinks he uses a genuine device, but instead is using the attackers system who record and pass the information to the real system so the user is not aware of it. This is used in ATM skimming equipment where the attacker replaces the input keyboard with there own. The observation can also happen from the outside where the observer by observing the interaction between the user and system during the authentication procedure is able to get enough information to later reuse it. This can be done by installing video cameras filming the key board and hand, or just by standing looking over the shoulder of the person authenticating and see what numbers that is pressed on the keyboard.

Security is not all about the technical solution, but also greatly depends on the user and the environment the system is used in. Today users creates there own security threat model witch is often very inaccurate [2] and because of different environmental situations they don't follow guidelines and recommendations they are educated to do [9]. Weirich and Sasse [2] conducted a study concerning various aspects of password security behaviour and some of the most important issues they found was that people think that if they follow good password behaviour they may be viewed as paranoid. Giving away there password may be viewed as act of trust to the other person. The users did not think they would be targeted and thought that criminals would not do much harm anyway. They also did not expect to be held responsible even if their behaviour did not comply with recommendation. In case of ATMs and payment terminals this may come from the fact that the banks cover the losses that we have with security incidents in most cases because it can not be proved that users behaved in a very inappropriate way. Weirich and Sasse [2] recommended using something they call 'fear appeals' to motivate users. This include punish the behaviour not the consequence and present the threat as a threat to there reputation.

For ATMs and payment terminals the major observation attack issue that is left is what is referred to as shoulder surfing [13]. Traditional approaches to fix this have been to create a plastic cover around the key pad and banks and credit card companies creating recommendation and guidelines to the users to cover the hand typing the PIN. Since we hope that our new PIN entry method provides better countermeasure against shoulder surfing attacks we want to take a look at what others have done to improve this. Some changes to the physical terminal location and physical design is the first defence that is done. The plastic cover should improve the defence at least from people standing slightly on the side. From our own experience it varies from ATM to ATM and terminal to terminal if they are equipped with this. Some ticket public access terminals have the payment terminal places inside a hole in the terminal that should make it harder to observe the pin entry. An study [9] of users in ATM found that only 35% did efforts to hid their PIN entry. So if the effort done on existing situations really work is not certain.

One approach that have been researched quite a bit to prevent shoulder surfing is the use of graphical passwords [43]. The idea that instead of having to provide a PIN Code or password we get to choose from a set of graphical passwords that we have earlier chosen is known to be easier to remember than normal PIN codes and passwords [16]. Graphical passwords if used directly where the user click or otherwise directly indicate the selected password it would be easy to observe the input for an attacker. Sakaria et. al [44] looked at shoulder surfing defence for graphical passwords and looked at tree different techniques for such system. Graphical password that also Fuglerud and Dale [16] mention has had quite some study and is know to be easier to remember that the normal PIN-code entry at least from a cognitive view. These methods is on the other hand not usable by people with visual disabilities. One system based on graphical images called 'The Convex Hull Click (CHC)' was presented by Wiedenbeck et al. [43] where the user instead of selecting a corresponding password has to recognize a set of pictures and create a mental convex hull that the pictures create and then click in this area. The convex hull is created at different areas for each login making observation attacks difficult.

Roth et. al [35] presented a method they refereed to as cognitive trapdoor games and probabilistic cognitive trapdoor games witch provides improved security against shoulder surfing attacks even when the attacker fully observes the pin entry or the pin entry is video taped and viewed later. They studied both the usability of the solution and the security. The system instead of letting the user enter the numbers directly presented the numbers on the keypad either with black or with colour. The number in the users pin code is presented in either white or black colour. The user instead of entering the number pressed a white or black button indicating that the number was in that group. It took about 10 times longer time to enter a PIN with there method than the regular way. After learned their method, it had about the same error probability as the regular method.

Different methods that use tactile feedback to the user during the authentication procedure to prevent shoulder surfing is done. De Luca et al. [10] presented a model VibraPass where the users cell phone was used to receive signals from the terminal during the authentication procedure. The terminal tell the cell phone to vibrate if the user should input a fake input. The input of the password would then consist of both correct and incorrect input. An observer would not by watching the authentication procedure one time be able to get the correct password as some of the values entered by the user was incorrect. Repeated observation of the user could on the other hand let the attacker get insight of what was the real password is. Sasamoto et al. [36] presented a model Undercover where a trackball on the terminal would give the user feedback on what picture to select. An attacker would not be able to observe the feedback to the user given through the trackball. From a universal design perspective giving the user tactile feedback could be positive. Tactile feedback has also been used with universal design and visual blind people [23]. Here they used special hardware with mouse buttons where the tactile markings can change to form a pattern, when the user moves the mouse over an item on the screen the pattern is presented as a tactile marking on the mouse button. They claim the security is enhanced, but the usability has to be improved as the authentication procedure took to long time.

Other approaches witch makes shoulder surfing difficult is EyePassword [24] where the user enters the password/pin by using there eyes. An camera that is able to monitor the eyes of the user is uses and it knows where the user is looking on the screen. This approach have the advantage that the normal PIN/Password can be used without being able to observed. Solution have multiple drawbacks making it less likely to be used in ATMs and payment terminals. Each uses has to be calibrated and stored in the system and obviously in our scenario can not be used with visual impaired users.

Most of the presented solutions require totally new hardware with new screens, cameras and input devices. Except the tactile feedback system witch my be usable by people with visual constrictions the solutions require that people don't have visual disabilities and to some extent not any cognitive problems.

2.3 Usability

Much work have been written and done on usability and human-computer interaction (HCI). HCI is concerned with how people use and interact with devices and systems that embed computation and how such systems can be more useful and usable [7]. HCI use concepts from both social and behavioural sciences and computer and information technology. HCI presents many different methods for how you should approach design process. Different methods that is used are checklists, guidelines, surveys, walk troughs and interviews, field studies and other real-world scenarios, laboratory experiments and various kinds of analytic methods [7]. One problem with some of the work of HCI when it comes to our study is that they focus a lot on our visual system [7]. When designing solution this is of course not a bad idea as most of our sensory receptors are visual receptors [7], but when it comes to universal design we also have to take into account people that does not have these receptors.

One model that has been used in HCI to evaluate human movement is a model called Fitts Law [7]. Carrol [7] argue that this model is the most successful of many to measure the human behaviour of information processing. Fitt's law [14] is used to predict the time it takes to move to a target area is depending on the distance and size of the target. This theory is used in many different disciplines and MacKenzie [27] describes it for use in HCI. A more detailed usage of the method related to our problem is to measure different text-entry rates on mobile phones [7] with different typing techniques. Our input method can not be used directly to compare it against the normal PIN entry method as Fitt's law as PIN entry both with our method and the normal people could use multiple fingers and both hands. If everyone used only one finger to press the keys it would be possible. Our method would then have advantages as the finger did not have to move so much between each keys and a drawback as we have more key presses than the normal method.

A more practical approach to usability design is a method from Cooper [8] where he focus on the target group and task and designing the solution with only them in mind. One thing Cooper [8] focus on is that adding multiple methods for operating the same things will add a higher cognitive fiction to the operation of the system. This is the same thing as when you let the ATM or payment terminal do more things than you would expect it to do. For instance withdraw money and do payments. Every new function added gives the user more choices, but also more choices for errors. This contradicts against what Fuglerud et al. [22] and Stephanidis [39] say about universal design as they say that the same system probably needs multiple ways of doing the same thing to support different user groups.

2.4 Safety and security

Brostoff and Sasse [6] identified Reasons [34] model as a good starting point when looking at security from a safety perspective. They demonstrated that Reasons concepts of active and latent failures offered an effective way of describing security issues that involved human behaviour. Safety and security has some common characteristics that is important, they are both secondary objectives. They are both there to protect the user when reaching their primary goal. Brostoff and Sasse [6] mention two of the biggest differences between safety and security as safety having a more obvious benefit to the user than security. With personal money transactions this may not be the case as most people are concerned that their money is handled in safely and that the payments is correctly. The second major difference is that safety does not have an active advisory who actively attacks as security have. For some reason people tend to not follow safety procedures and even when there is clear descriptions and hits about how to behave safe [9] people do not follow them.

2.5 Evaluation models

As we see above different models for designing usable solutions [8] [7] and the connection between security and safety [6]. Helkala and Snekkenes [21] presented one model for ranking authentication solutions that include the user ability to use the system and the environment. The evaluation is here done in a four step process where all available authentication products is evaluated. The four steps is 1. User and environment compatibility, 2. Security level compatibility , 3. Usability and 4. Costs. In the first step if all available solutions is evaluated if they support the requirements for the scenario. If they do not they are removed and not taken further to step 2. In our scenario with public access terminals that should be usable by as many as possible this model does not fit well. Another evaluation model of authentication solutions that directly includes disabilities scenarios is presented by Renaud in[18]. In this model the solution is evaluated for accessibility, memorability, security and cost. Accessibility consist of tree parts: special requirements, convenience and inclusivity. Here inclusivity is considered based on tree types of disability: sensory, physical and cognitive. Depending on how many of the tree disabilities an solution have the larger deficit the solution have. Other categories are evaluated to how much deficit they constitute. The model consider both disabilities and security but does not look closely at how these factors may influence each other.

3 Universal design

Different definition and terms is used to describe universal design. 'Design for all', 'Inclusive design' and 'Universal Access' is all terms that is used, but with slightly different meaning. Universal design was first used by Ron Mace [**?**] and is the term most common in USA. Design for all is common on EU. Universal design, design for all and inclusive design are all trying to describe how we should design solutions for use in everyday life so that all people, regardless of disability, age, race, cognitive skill and so on can use them. Stephanidis [39] uses the term universal access as approaches to accessibility to computer based applications used by users with disabilities. Universal access is more limited then universal design in that the latter also takes into account the environment the system operates in.

One of the most used definitions of universal design comes from The Center of Universal Design at the University of North Carolina and they define it like this [15]:

> "*Universal design is the design of products and environments to be usable by all people, to the greatest extent possible, without the need for adaptation or specialized design. The intent of universal design is to simplify life for everyone by making products, communications, and the built environment more usable by as many people as possible at little or no extra cost. Universal design benefits people of all ages and abilities.*"

Another definition is given in the United Nations Convention on the Rights of Persons with Disabilities [29]

> *"Universal design" means the design of products, environments, programmes and services to be usable by all people, to the greatest extent possible, without the need for adaptation or specialized design. "Universal design" shall not exclude assistive devices for particular groups of persons with disabilities where this is needed. Universal design is not about making special solutions for people with disabilities, but to design solutions that are usable by as many as possible. The UN definition states clearly that Universal Design does not exclude assistive devices.*

3.1 History

In the beginning of the 19'th century people with disabilities was not taking part in society as they are today and we did not live as long as today. After the Second World War many veterans returned with disabilities like lost limbs, wheelchair and so on and it became more important to include these people into society. Universal design first came out from architecture and building design where public areas and houses should be made accessible also with people with different kinds of physical disabilities. One of the first examples where universal design was used was on curb cuts. They where first introduced in the US in the forties to help people in wheelchairs, but today we see the benefit for everyone when we are using bicycles, roller blades, children trolleys and shopping trolleys.

Today universal design is part of the legislation in Norway and is part of the law against discrimination against people because of disabilities [26]. Here the law states that this includes both architecture and ICT system that is used by the public. New ICT system should be designed with universal design in mind from 1. June 2011 and old system should be changed by 1. January 2021.

3.2 Principles

'The Principles of Universal Design' [15] [1] developed by The Center of Universal Design is a set of seven principles with guidelines to universal design and is listed below. They state that these principles can be used to evaluate existing designs, guide designers in new designs to make products and environments more useful for everyone.

PRINCIPLE ONE: Equitable Use

The design is useful and marketable to people with diverse abilities.
Guidelines:
1a. Provide the same means of use for all users: identical whenever possible; equivalent when not.
1b. Avoid segregating or stigmatizing any users.
1c. Provisions for privacy, security, and safety should be equally available to all users.
1d. Make the design appealing to all users.

PRINCIPLE TWO: Flexibility in Use

The design accommodates a wide range of individual preferences and abilities.
Guidelines:
2a. Provide choice in methods of use.
2b. Accommodate right- or left-handed access and use.
2c. Facilitate the user's accuracy and precision.
2d. Provide adaptability to the user's pace.

PRINCIPLE THREE: Simple and Intuitive Use

Use of the design is easy to understand, regardless of the user's experience, knowledge, language skills, or current concentration level.
Guidelines:
3a. Eliminate unnecessary complexity.
3b. Be consistent with user expectations and intuition.
3c. Accommodate a wide range of literacy and language skills.
3d. Arrange information consistent with its importance.
3e. Provide effective prompting and feedback during and after task completion.

[1] Copyright © 1997 NC State University, The Center for Universal Design.

PRINCIPLE FOUR: Perceptible Information

The design communicates necessary information effectively to the user, regardless of ambient conditions or the user's sensory abilities.

Guidelines:

4a. Use different modes (pictorial, verbal, tactile) for redundant presentation of essential information.
4b. Provide adequate contrast between essential information and its surroundings.
4c. Maximize "legibility" of essential information.
4d. Differentiate elements in ways that can be described (i.e., make it easy to give instructions or directions).
4e. Provide compatibility with a variety of techniques or devices used by people with sensory limitations.

PRINCIPLE FIVE: Tolerance for Error

The design minimizes hazards and the adverse consequences of accidental or unintended actions.

Guidelines:

5a. Arrange elements to minimize hazards and errors: most used elements, most accessible; hazardous elements eliminated, isolated, or shielded.
5b. Provide warnings of hazards and errors.
5c. Provide fail safe features.
5d. Discourage unconscious action in tasks that require vigilance.

PRINCIPLE SIX: Low Physical Effort

The design can be used efficiently and comfortably and with a minimum of fatigue.

Guidelines:

6a. Allow user to maintain a neutral body position.
6b. Use reasonable operating forces.
6c. Minimize repetitive actions.
6d. Minimize sustained physical effort.

PRINCIPLE SEVEN: Size and Space for Approach and Use

Appropriate size and space is provided for approach, reach, manipulation, and use regardless of user's body size, posture, or mobility.

Guidelines:

7a. Provide a clear line of sight to important elements for any seated or standing user.
7b. Make reach to all components comfortable for any seated or standing user.
7c. Accommodate variations in hand and grip size.
7d. Provide adequate space for the use of assistive devices or personal assistance.

3.3 Motivation for universal design

There are multiple reasons why we should design with universal design in mind. The Norwegian Law against discrimination [26] talks about equal rights to participate in society for everyone regardless of disability. The benefits for the user to be able to participate and use is obvious, but it could also have an economical benefit for governments as less money can be spent on welfare as more people is able to participate in society and be more integrated. Vendors and owners of systems designed with universal design can also benefit as the public opinion can give them more credibility. Good design could also reduce cost, for instance could the amount spent on training be reduced.

One important principle with Universal Design is that is not specifically design for one particular group of people with a disability. All users should benefit from it. Solutions designed for people with visual impairments in mind could benefit everyone where the lighting conditions is not good for instance in darkness. Solutions designed for people with hearing impairments would benefit everyone when operating thing in very noisy environments.

One last benefit that we hope Universal Design can provide is by thinking outside the box and creatively because we have to see things from other people's minds that have problems most of us don't have we may come up with solutions that solve other problems that what they originally was not design to solve. One example where this has happened before is with the design of the first hearing aid. The device had to be so small to fit behind the person's ear and at that time the electronic devices was large. One of the first commercial usages of the transistor was in hearing aids for hearing impaired users in the early 50ies. Even though the transistor was not invented directly to solve the problem with hearing aid it became one of the most important inventions in the 19th century.

4 Public access terminals

This chapter takes a look at public access terminals (PAT) and describes the work done both from an universal design perspective and from a security view. This paper focuses on two particular types of terminals that according to [39] is part of a class of transactional public access terminals where the purpose is to execute an economical transaction. First we describe the public access terminals in general before we go on and look at the more detailed ATM and payment terminal.

A public access terminal can be defined as a information technology based interactive system, located in a public area [39]. The terminals can be located both indoor and outdoor, used by all people, providing access to information or sales of services and products. The terminals can store information locally or be connected to a network. There exists a large range of public terminal types, but they can be divided into two main groups, information public access terminals and transactional public access terminals.

Information public access terminals:
These terminals are interactive terminals that accepts interaction from any user and does not demand any form of authentication or identification. They are often used in transportation areas, museums, tourist information centres, building information and so on.

Transactional public access terminals:
These terminals are used to carry out financial transaction for buying goods or services without the help of a clerk. They can be further divided based on there usage into more categories based on there specific usage. Financial transaction PAT's requiring authentication like ATMs and payment terminals. Financial transaction PAT's without user authentication like ticket machines, parking machines and vending machines. Non financial PAT's with user authentication like voting machines and non financial PAT's without user authentication like job application kiosks. We also have hybrid terminals that supports both payments with authentication and without and some transactional PAT's that is also information kiosks like some travelling ticket systems.

The oldest and maybe most common PAT is the automatic teller machine (ATM). ATM's can be a wall mounted or standalone banking terminal that bank customers can us to make bank transactions. In Norway the most common usage of these terminals is to withdraw cash, but some other services like viewing account transactions, withdrawing different currencies and recharging cell phone cards is also available in some locations. In other countries other services is also provided like check deposits, bill payment and transfer money between accounts. Most ATM is connected to a global banking network to make it possible for one user in one country to use ATM's all around the world. The second large group of transactional PATs are payment terminals that is placed in stores and restaurants and provides payments for goods and services. These terminals is also connected to the world wide banking system so transactions can be provided all around the world. Payment terminals also exists in different forms and functions, some are mounted to the cash system in stores, some are wireless and rely on wireless communication to connect to the back end banking system. Some work off line and can later be connected to the banking network like payment terminals used in air planes.

4.1 User interaction

User interaction with PAT's can be grouped into four different categories [39] :

1. Physical/environmental
2. User authentication
3. Operation
4. Cash/money handling

Issues connected to physical/environmental includes the size and hight of the terminal, the type of enclosure like stand alone, wall mount and drive-ins. User identification is in most cases done with inserting a plastic card with magnetic strip or smart card into a card reader. The most used authentication method is still mostly done with entering a 4 digit pin code into a numeric keypad. The main operation of PATs include different input devices like touch screens, number key pads, function keys , trackballs, keyboards, bar-code readers and bill scanners. Output devices consists of display screens, receipts printers, speakers, headphone jacks and other kinds of printers. Cash/money handling is done with bill and coin dispensers and cash/check deposits.

4.2 Usability and accessibility issues

Since these terminals is used by so many people with different background, training and skills extensive research and investigation have been done the last decades to improve the general usability and accessibility of PATs. Different national guidelines/check lists have been created to further help designers to create better solutions [40]. International standards from ITU [20] and EU [12] describes both security and usability issues in regards to public access terminals and pin entry. With all the standards and guidelines available it's still many issues with such terminals. The terminals is created often with the exact same purpose, but the design can differ quite a bit. There is also an contradiction with some of these guidelines that suggest that the terminals should be able to use with only one hand, but where security recommendations from banks and credit card companies suggest that you should cover the hand used with the second hand.

4.3 Universal design

Different techniques to improve the accessibility has been suggested. Kouroupetroglou [39] lists some suggested directions and techniques like voice output, create a separate audio menu. Tactile indicators to buttons and keys. Raised buttons so they are tactile. Take a close look at text size, colours and contrast both in the display and on the keys, don't use colour for meaning and use the telephone layout for the number keys not the keyboard layout. Some of these techniques are found in many ATMs and payment terminals like tactile indicator and raised buttons. Tactile indicators vary between different terminal types and many uses green, yellow and red for the control keys. Raised buttons is different and even the key layout is different between vendors of such devices. In Norway some ATM's is equipped with voice output [16], but is only placed in a few ATM from two different banks. Some terminals use audio feedback when pressed and some don't, most terminals have a lot of extra keys that most people never use. Examples of payment terminal designs is shown in Figure 1

4.4 Security

Security of ATM's and payment terminals is an important issue as they handle large amount of transactions and money. Improvements to the terminals is an ongoing process and the banks and credit card companies continue to improve them to lower the theft, robbery and misuse of them. We will here only describe the security improvements to the physical environment, and treat the terminals as a trusted device. It's no doubt that the terminal itself with the software, communication protocols and so on is very important to secure and it's probably an ongoing process to also make sure that this part of the system is also continuous improved and tested. One of the biggest threats to these terminals is that they are placed in public areas where they can be accesses by everyone, both the user itself and by third parties trying to exploit them. Different ways of exploiting the system has been used, like ATMs modified with skimming equipment. Skimming equipment exists in different forms and levels. From an simple add-on to the card slot of the ATM design to just steal your credit card when you insert in the card slot, to more advanced where the entire front panel of the ATM is changed with new keypad, card reader and even video cameras. For payment terminals in stores and restaurants unfaithful workers may have separate card readers to copy your credit card information when you give away your credit card to make the payment. Security issues of course also exist when there has not been done changes to the physical devices. The plastic card together with the pin code is all that a thief needs to empty your account. Keeping the credit card safe so it does not get stolen is of course important. The thief also would need the pin code to use the card and we are told not to write down the number and keep it together with the card. The pin code can be stolen by people watching you entering the pin code on the terminal. This is called shoulder surfing. Different methods of this exist as we explained with more advanced skimming equipment where video cameras filming your hand, to people behind you look over your shoulder and see what you enter, with video cameras or binoculars this can also be done from an distance if the placement of the payment terminal/ATM is in such a way. In Norway this has been reported the case in train ticket machines in railway stations in Oslo [41].

The biggest security improvement to these systems are probably the introduction of smart card chips on the plastic cards with new smart card readers on the terminals. This made it much harder for criminals to read and copy the credit card information. In Norway all cards are equipped with this today, but the magnetic strip is still on the card with the information. The magnetic strip can be used as an backup solution if the smart card reader does not work. When using the same credit card in other countries it's not always working to use the chip and we have to rely on the magnetic strip. ATMs are also been equipped with anti skimming equipment making it harder to install such devices, but criminals still find ways to bypass them [4]. Both ATM and payment terminals is often equipped with plastic covers around the key pad making it harder to see what the user is typing.

De Luca et al. [9] did a field study on the usage of ATMs and found some interesting discoveries related to security. Even with both guidelines how to avoid security incidents when using such terminals people did not follow them. In the field study they discovered that over 65% did not hide the input of the pin code or did so weakly. Different reasons for this was found like carrying bags, talking to people while operating the device. It looked like the social setting where the terminal is used has an large impact on how people interact with these systems. The security of the device, rules and procedures may not be enough to provide good security for these public terminals.

5 Evaluation model for authentication solutions

In this chapter we describe a model for designing authentication solutions with universal design in mind. When designing new products and solutions usability guidelines suggest that we should identify the user group that we want to design for [8] and focus on the task that group should accomplish with the solution. When creating solutions with universal design in mind we have to take all user groups into consideration, and it's therefore a bit different. Fuglerud et. al [16] suggests that the solutions must adapt and change depending on the user group. This is what is called 'adaptive user interfaces' [25]. Another model [32] have looked at it from a usability-accessibility viewpoint where the user interface consist on different modalities and instead of focusing on the individual users handicap they refer to it as a constriction on their usage of the interface. This is described as multimodal interaction where the user interface has multiple modes of operation. Constrictions to the usage do not only come from the user itself, but also from the device, environmental and social settings. When referring to it as disabilities it has a more negative tone than talking about constrictions. Constrictions are a more general term and we all may have constrictions to our use of a system for instance could stress influence our cognitive and perception skills. When combining this with normal Human-Computer-Interaction (HCI) interactions new interconnection can be spotted. This design method could lead to better usability, but as Obrenovic et. al [32] says it can also be very valuable to people without disabilities using the system under suboptimal conditions. Because of this effect we also hope that this model will lead to information that would improve the general security of the designed system. Observation attacks on authentication solutions uses information gathered through watching the interaction between the user and the system and the observation is also affected by the same constrictions. Often when it comes to security incidents with authentication solution the user is blamed for not following procedures or not paying attention. Giving away or having a written note with the pin code in the wallet is a good example. On the other hand when blind people says they have given away there pin code and card to third parties we don't consider this a bad thing by the user, but instead blame the system. Fuglerud [17] says that as so many as 45% of visual impaired in Norway have given away there pin code and 28% in payment terminals. This type of thinking where the user is blamed is similar to the 'old-view' of human error problems [11] that was normal in the 80ies.

An example from payment terminals with multi modal interfaces could be the fact that they support both magnetic stripes and smart card for identification of the card. This duality is not made for that, but instead made to be backwards compatible. But as an example of the same small device supporting multiple interfaces is serves it purpose. The Norwegian ATMs that is equipped with microphone jacks and have an alternative sound menu instead of the normal lcd screen is an true example of multi modality. Maybe the same thing can be done with the pin entry method to support both different user with different constrictions and to be used in different situations.

5.1 Usability and accessibility through modalities and constraints

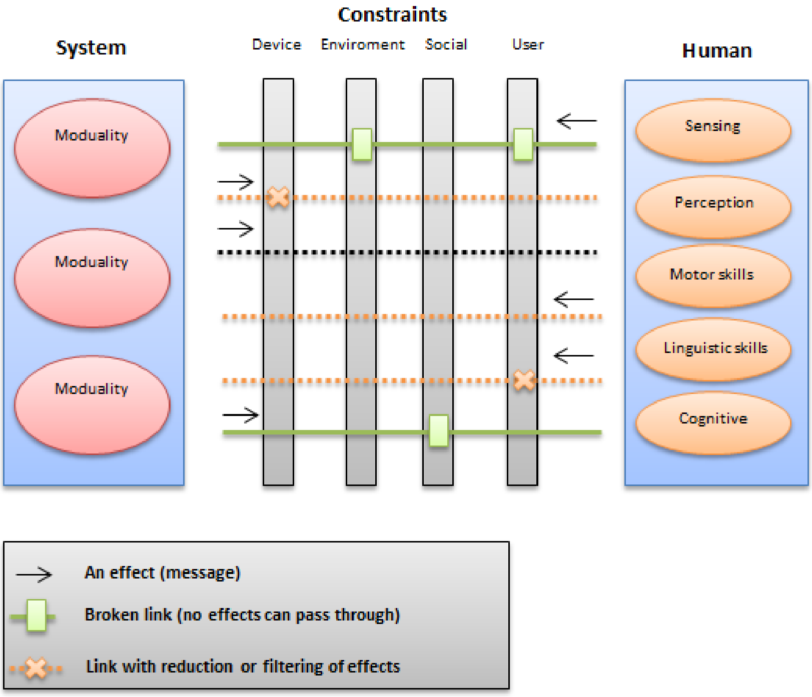


Figure 2: Modalities, constriction and effects [31]

Back to the model from Obrenevic et. al [32] the model describes the user interface as a set of communication channels from the system to the user and from the user to the system. These channels may be broken or have reduced or filtering of effects because of different constrictions. They use four different types of constrictions, device constrictions, environmental constrictions, social constraints and user constrictions. Their framework does not define any specific system interaction modality or any user constraints like low vision, hearing problems, but a more generic unified view of describing such a system. This makes it useful to use it on any kind of device user interaction situations. The model is based on the idea that the interface can be viewed as a higher order message sent from the designers and from the user back to the system. An input modality requires a device to transfer human output into a form suitable for computer processing. This could be a keyboard, touch screen or voice. In our example when looking at an ATM's it usually have multiple output and input modalities. Output modalities would be the screen, receipt printer and where you get the cash. Input modalities would be the keyboard, card insert slot and often some separate keys next to the screen to do selection. Some ATM's [16] has even added a separate speech output modalities to help visual impaired. Their model handle different kinds of input modalities where some could be streaming (like voice recognition) and event based input like keyboards. When looking at these modalities they describe various interaction constraints that could happen on these modalities. Constraints can be viewed as filters on usage. In Figure 2 both modalities, constraints and effects is displayed. We argue that the two last constrictions, social and user are also affected by other constraints described in human error theory. Human error theory argues that we should not blame the user, but look more on the system and organizational side of the system.

5.2 Security

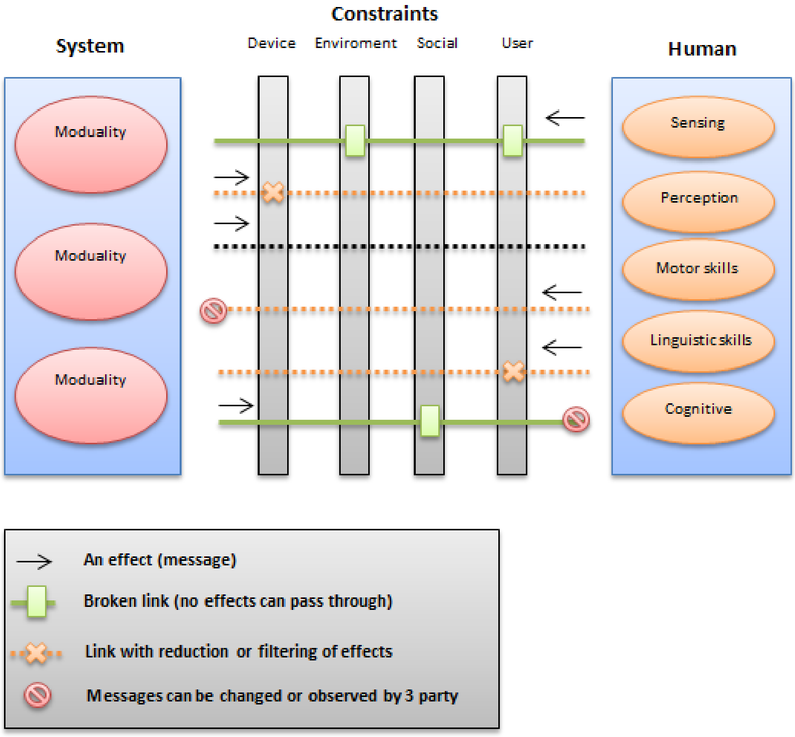


Figure 3: Our modified model where messages can be observed.

When looking at it from a security perspective the signals sent from the system and user can be intercepted or changed by a third party to gain insight and manipulate the information sent between the user and system. The same constraints and filters that apply to the normal user may apply to a third person trying to gain insight. We therefore expand the model and look at how the effects can be viewed, changed and stopped by a third party who wants to use the information to gain unauthorized information. In Figure 3 both modalities, constraints and effects is displayed. The interception of messages sent back and forth between the user and the system is also displayed. The observation could be done both on signals created by the system or by the user. The signals could be intercepted and retransmitted in real time without the user or system noticing it like it is when the card reader is replaced with a fake one in skimming equipment or the signals can just be observed and used later to gain access like it is with shoulder surfing. The different modalities may also leak information though other channels than what was though of by the designer of the system. For instance in an ATM the card reader makes a sound from the physical reader when the card is inserted and when the card is returned from the reader.

A blind person could use this information to know when the card is returned instead of relying on his vision. In the same way from a security perspective these new modalities could also by used by an third party to gain unauthorized information from the system. For instance could the buttons make sounds when they are pressed that could be used to Figure out witch key was pressed.

To include security into the model there are multiple things we have to look at. First the signals sent to and from the user in an authentication solution can be monitored, changed and intercepted by a third party. The first thing we have to do is to look at each of the signals and see how and what an third party could to with it. Can for instance the information interception be used to get unauthorized access later or is it feasible to replace the signals with new signals. All the constrictions also apply to a third party and by looking at the signals back and forth between the system and the user we will be able to notice if these signals can be monitored or intercepted by a third party.

5.3 Security and safety

Security and safety have many similarities. Both are in most cases secondary objectives when using or operating a system. In our case when looking at payment terminals and ATM's the main objective is to pay for the goods or in an ATM to withdraw money. Security is on both cases important, but it's not the main objective. In our model we enhance the model by Obrenovic et. al [32] to also take security into consideration. We argue that there are more constrictions that those mention by Obrenovic et. al [32] to the usage of a system, but as they say the model is generic and can be expanded with more constrictions. From a human error perspective [11] our usage of a system is also affected by many other factors like cognitive fixation, plan continuation, stress, knowledge, new technology, automation surprises and procedural adoption that all influence our usage of the system. Our model will only cover the security on the interaction between the human and the system and will make an assumption that the computer equipment / device is a trusted device. Sasse et. al [37] argues that there is a distinction between safety and security in the way that safety failures are frequent accidents, but security incidents often are deliberate and are likely to happen again and again. As they argue this point is greatly reduced if we look at the world we live in as a dangerous place.

5.4 Errors and violations

From safety theory it's important to disquisition between errors and violations [34]. The same topics is important to take into consideration when designing authentication solutions. Humans are always involved and even if we design a system to take this into consideration humans makes mistakes. The world and the humans that use the system is a complex place and the situation your solution in used in can be very different. Reason [34] further divides errors into unaware deviations of actions from intentions and the deviation from the normal path toward a desired goal. The first two, Reason calls slips and lapses and the second is mistakes. This types is not enough to get the full picture. Humans operate in a social context and there is therefore important to understand that there is more to it than the way they do the task. Errors is more related to human cognitive processes, violations is better described as a deliberate deviation from the security procedures that is given by the operators, designers and management of the system. The violations does not have to reprehensible. For instance we know that we should cover the pin entry when typing the pin in an ATM, but people still don't do it. Also giving away our pin code to others is also viewed as a violation. We argue that for people with disabilities we view these violations as less reprehensible. Much of this work on safety is based on work in very complex system, but as we said earlier if we view the world as a complex and dangerous system these principles on errors and violations fits in also with information security. More people [6] have recognized this and found many connections between safety and security. There are both similarities and differences, but when designing the solutions we should try to identity different types of errors and violations a human can end up doing when using the system and why. In Figure 2 Reason [34] summarizes the different unsafe acts classifying into intentional and unintentional. One or two simple mistakes may not cause a security incident by them self, but in certain situations they may together

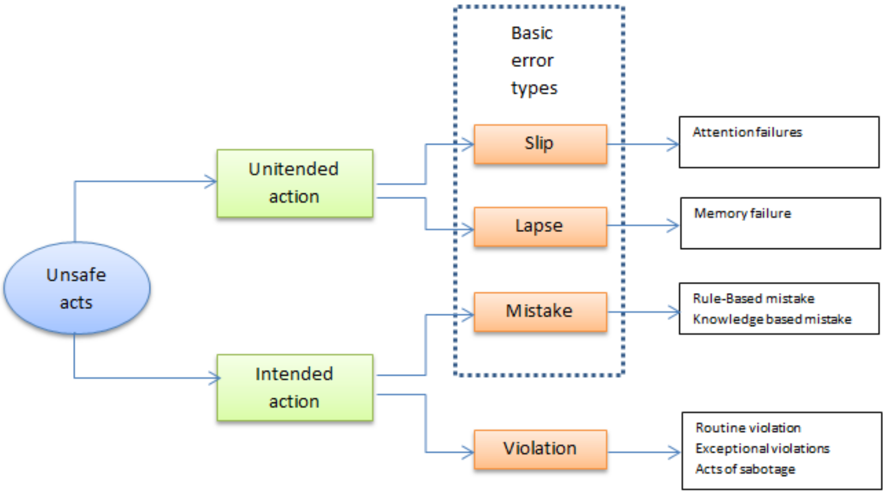


Figure 4: Actions classified if they where intended or unintended and errors from violations [34]

In the next Section we look at what normally goes wrong when people interact with a system. This may help us identify more problems with solutions we are designing.

5.5 What can go wrong?

When looking at what can go wrong and what security incidents that can happens with our designed solution we may use the work from Dekker [11] on human error and look at it from different angels. Dekker [11] lists different mechanisms that may lead to error and in our case security incidents.

5.5.1 Cognitive Fixation

When looking at why incidents happens it's often easy to start saying, 'Why did the user not see this', or 'why did he not notice it?'. We only now this afterwards in hindsight and it does not explain what the user went through when it happened. With routines or things we do a lot like with authentication solutions we are fixated at what is the normal routine. This may distract us when something unexpected happens and people may be fixated on the situation.

5.5.2 Plan continuation

When unexpected things happens we still want to complete the original plan. In a setting with authentication solutions the user will try to complete the procedure even if he noticing that something unexpected or wrong is about to happen. The user will try to complete the authentication procedure even if he was distracted. When for instance the user is in front of a ATM that is equipped with skimming equipment the user may sense that something is different or wrong, but he is still sticking with the plan to authenticate and get the job done. Here we have to Figure out why people stick to the plan and make the solution stop or inform the user.

5.5.3 Stress

Stress is another situation that may lead the user to not follow procedures. As reported by [9] users in an ATM seemed to behave differently when there was a line behind them. This may be because the situation made it more stressful. Stress also cause tunnelling. People tend to focus only on the job when stressed and filter out other signals. Stress also cause distortion of time. In an authentication situation the user will try to do the procedures faster than he normally would when not under stress. From our own experience this happens in payment terminals when there is a long line and people want us to finish quickly. We may try to do the authentication procedure faster and forget to follow procedure. Other factors like fatigue also affects users, in a safety work this can maybe be controlled by the organization by not letting there workers be tired and worn out, but for authentication solutions used by everyone at any time it's impossible for the owner of the equipment to control the users.

5.5.4 Knowledge

Dekker [11] describes that people needs tree things to apply knowledge to manage situations. They need to possess the knowledge, they need to have the information organized to cope with the situation and they need to be able to activate it in the right context. Authentication solutions is created to be self explanatory and how to use the pin code is never thought only assumed that people understand how to use it. There is a lot of steps a users can do to if they know. For instance use a ATM in a secure matter, using it outside a bank is more secure than other places because there are video surveillance, using it in day light instead of at night because of robbers and many other situations. But not all users possess this information. The organizations in charge of these solutions need to give the users this knowledge as they can't expect the user to figure out this by themselves.

5.5.5 New technology and computerization

When introducing new technology it can lead to less security incidents, but introducing new technology may also lead to new unforeseen consequences. In Norway most ATM's and payment terminals now uses a chip instead of the magnetic stripe on the card to identify the user. This new technology improved the security by making it a lot harder for 3'parties to copy the information from the card. Other technology improvements like wireless terminals made it easier for instance restaurants to bring the payment terminal to the user by his table so he would not have to give the waiter the card. This made copying of card information harder as the card never leaves the sight of the user. Some new payment terminals is now equipped with touch screens instead of real buttons, this may make it harder to equip the terminals with skimming equipment, but it makes them useless to visual impaired users. Usually the buttons light up when they are touched on the screen to make visual clues to the user, but it also makes it easier for shoulder surfers to see what button the users was pushing.

5.5.6 Automation surprises

This happens when the user think the operation is in one mode, but the system is actually in another. To make the user less likely to make errors it's important to be consistent with what the user expect the mode to be and not introducing something different without a clear indication about the mode. Even with simple processes like using payment terminals this can happen. For example in some restaurants they want the user to type the total amount to apply extra tip. Since the normal procedure is to provide only the pin code and not the total amount, the pin code may be entered as the total amount this amount is displayed in clear text and the pin may be observed by others. This also happens in other authentication solutions where the user have to enter both an identification and a password. If the user is not paying attention to what field he is entering the information in the password may be entered in the user name field and the password is displayed in clear text on the screen.

5.5.7 Procedural adoption

People don't always follow procedures and there may be many reasons for that. When a system is designed we tend to create it with a clear understanding of how we expect the user to use it. The world is a complex place and when designing the system we can't take into account all external things that can influence the user when accomplishing the designed procedure. The situation the user was in can lead to for instance distraction making the user forget or adapt to the situation and by that not following the designed procedure. We often look back at these situations with hindsight and think that why did the user to that. When looking at why people don't follow procedures we have to look at the reason behind it and not blame the user for "procedure violations" and "non-compliance".

5.6 Applying the model

To really see what can go wrong in the usage of the designed system you have to avoid looking at the things that goes wrong from the outside. This is only good for hindsight. Instead we have to put ourselves into the situation the user faces when uses the system and look at things that might happen. When dealing with universal design this can be extremely difficult as the users of the system may have challenges not visual to the designers. We start with describing all the modalities the designed system uses and what effects the modality uses. We can start at a high level and divide this further into more detailed modalities. Then we look at each user group and how different disabilities reduce some of the effects of the interaction with the system. We can do this in two different ways, take the normal user without any reduced effects and create profiles for each user group with disabilities and describe which effects is different than for the reference group. Or the other way where we describe each group with the affected effects. Next step is to look at each of the constraints related to the device, environment, user and social and how they influence the usage of the effect. For social and user constraints we also use Dekker's [11] where human error could cause errors and incidents to happen. For identified errors we then create an table where we look at what type of error this is according to Reasons [34] error types. For observation attacks on authentication solutions we also look at each modality the system uses and see how and if the effect can be observed either by the intended effect or by some of the side effects. In the next chapter we will use these guidelines to explain both how this looks at for our payment terminal and today's ATMs.

In the next chapter we will take a look at how the model can be used on a payment terminal using the regular PIN entry method.

6 Using the evaluation model on a payment terminal with the old PIN entry method

The first step in using the model on a payment terminal is to describe the user interface as a set of modalities. We have both input and output modalities, the keyboard is of course the most important input modality and the screen is the main output modality. The smart card reader and magnetic stripe reader is also input modalities. We divide the keyboard into two sub modalities to further identify issues with it. Some payment terminals have back light on the keyboard and if it had we would add that to the keyboard modality.

Modality	Composed of	Effect which the modality use	Effect type
Keyboard	Numeric keys	Hand movement	Motor
Keyboard	Numeric keys	Pressure	Motor
Keyboard	Numeric keys	Shape recognition	Perception
Keyboard	Numeric keys	Tactile marking	Sensing
Keyboard	Numeric keys	Numbers	Sensory and Cognitive
Keyboard	Control keys	Hand movement	Motor
Keyboard	Control keys	Pressure	Motor
Keyboard	Control keys	Shape recognition	Perception
Keyboard	Control keys	Color recognition	Perception
Keyboard	Control keys	Tactile marking	Sensing
Keyboard	Control keys	Text	Sensory and Cognitive
Card reader	Smart card reader	Hand movement	Motor
Card reader	Smart card reader	Shape recognition	Perception
Card reader	Magnetic stripe reader	Hand movement	Motor
Card reader	Magnetic stripe reader	Shape recognition	Perception
Display	Letter	Normal vision	Sensory
Display	Word	Shape recognition	Perception
Display	Sentence	Grouping of words	Perception

Table 1: Modalities and effects they use on a payment terminal

In Table 1 we list them with the effects they use. We added both color recognition and sound recognition as effects as many terminals uses color to distinguish control keys and sound to indicate a button is pressed. Because these effects is easy to understand when we show how different effects are reduced because of different constrictions it's part of our table. We also add the card input slot and the card magnetic stripe reader that we would find on a typical payment terminal as an modality in the user interface of the payment terminal.

We then have to look at what effects are absent or reduced by different disabilities. Table 2 show examples of what effects different disabilities gives [32]. This list could be expanded

Disability	**Effect reduced by disability**
Blindness	Absence of all visual stimulus processing
Poor acuity (poor sharpness)	Reduced visual sharpness
Clouded vision	Reduced visual sharpness
Central field loss	Reduced central vision
Color blindness	Reduced color sensation and contrast processing
Deafness	Absence of all audio stimulus processing
Hard of hearing	Reduced audio sensory processing
Muscular weakness	Reduced movement and pressure
Limitation of muscular control	Reduced movement
Limitation of sensation	Reduced pressure
Joint problems	Reduced movement
Pain associated with movement	Reduced movement
Dyslexia	Reduced linguistic effects
Attention Deficit Disorder	Reduced attention
Memory impairments	Reduced memory processing

Table 2: Examples of disabilities with constraints and effects [32]

Constraints	**Situations (sub constraint)**	**Influence the usage of effect**
Smart Card reader	Card inserted wrong	Can only be read if the card is inserted correctly
Magnetic stripe reader	Card used wrong way	Can only be read if the card is moved with the magnetic stripe the correct way.
Magnetic stripe reader	Card with smart card	Magnetic stripe can not be used.
Key pad		Can not be used to type letters.

Table 3: Device constraints using the payment terminal

with more effects and disabilities as described in [39]. Blindness would give absence of all visual stimulus and muscular weakness could mean that hand movement would be limited.

Next step is to look at how different constraints affect the usage of different effects. We look at these constriction from different angels as described in the Figure 2. In Table 3 we look at constraints in regard to the device it self, Table 4 we look at environmental constraints. Since constraints caused by the environment depends on where the payment terminal is operated we should look at constrictions that may apply because of the setting it is used. For instance in an pub where the lighting conditions can be low it have effects on modalities where we dependent on visual interaction. Table 6 show user constraints and 5 we list different social constraints.

We then create a list of all errors we think the user is capable of doing related to social and user constraints and map them to the modality it uses if applicable. We also classify the errors according to Reasons model [34] and use Dekkers [11] points on what can go wrong to describe it.

Constraints	**Situations (sub constraint)**	**Influence the usage of effect**
Visual condition	Good lighting	No specific reductions.
Visual condition	Dim lighting	User has to be more focused on where to press keys.
Visual condition	Dark	User can not rely on vision to use terminal.
Noise level	Quiet	No specific reductions.
Noise level	Normal noise level	Can be used if sound used are at appropriate level.
Noise level	High noise level	All audio effects are reduced.

Table 4: Environmental constraints using the payment terminal

Constraints	**Situations (sub constraint)**	**Influence the usage of effect**
Number of people	Alone	No specific reductions.
Number of people	Crowded	Attention may be reduced. Noise higher. Cognitive fixation
Number of people	With someone else	Attention may be reduced.

Table 5: Social constraints using the payment terminal

Constraints	**Situations (sub constraint)**	**Influence the usage of effect**
Blind		Absence of visual effects.
Dyslectic		Linguistics skills reduced.
Deaf	Sound used as feedback	Absence of sound effects.
Affected by drugs		Memory, motor and perception skills like attention reduced.
Affected by alcohol		Memory, motor and perception skills like attention reduced.
User state	Relaxed	No specific reductions
User state	Stressed	Tunnelling, linguistics and perception skills like attention reduced. Distortion of time
User state	Cognitive fixation	Percept ion skills like attention reduced. Act on instinct instead of thinking.
User state	Plan continuation	Perception skills like attention reduced. Act on instinct instead of thinking.
Knowledge	Good	No reduction
Knowledge	Average	Lower cognitive and perception skills as they don't remember what to do.
Knowledge	Low	Cognitive and perception skills reduced because they don't have the knowledge.

Table 6: User constraints using the payment terminal

To further evaluate the security trough the model we have to look at each of the modalities and see how information can be observed, used or manipulated when the effects pass from the

Error type	Situations	Affected modality
Slip	Writes the PIN code instead of amount.	Keyboard, screen
Slip	Removes the card before transaction finished.	Card reader, screen
Lapse	Forget the PIN code and writes a wrong PIN	
Mistake	User does not cover the input as recommended and PIN code gets observed..	Keyboard
Mistake	User writes down the PIN code and keep it together with the card and someone gets hold of both and misuse it.	
Violation	User does not check for skimming equipment or terminal manipulation.	Keyboard, card reader and screen.
Violation	Uses a stolen credit card and try to use it.	Keyboard, card reader and screen.

Table 7: Identified errors, mapped to error type and affected modality

Modality	Side channel	How	Risk/Weakness
Numeric keys	Visual	Observer can see the hand movement and see what key is pressed.	Get the PIN code
Numeric keys	Sound	Observer can by listening to sound from keys to know what is pressed.	Get the PIN code
Numeric keys	Movement	Observer can see the movement of the keys as they are pressed.	Get the PIN code
Control keys	Visual	Observer can see the hand movement and see what key is pressed.	Know when user is finished typing PIN
Control keys	Sound	Observer can by listening to sound from keys know what is pressed.	Know when user is finished typing PIN
Control keys	Movement	Observer can see the movement of the keys as they are pressed.	Know when user is finished typing PIN

Table 8: Security issues connected to modalities.

system to the user and from the user to the system. Each of the modalities may also send signals through other channels than the designer thought of and we also have to look for them and how they can be observed. In Table 8 we list the ones we can identify. The same constrictions that apply for a user may also affect how easy it is to observe. For instance if its dark or the person who is shoulder surfing have visual disabilities it will make it difficult to observe the PIN entry.

Blindness stops all messages that is sent and received by modalities that uses visual stimuli. We can try to close our eyes and think how a blind user may approach the system for the first time, or try to operate it when there is no light. The user would start by using her hands to touch the terminal to make a mental picture of how it looks and should be operated. If she does not have any prior knowledge on how to operate the terminal it will not be self explainable. Seeing people would have been able to observe how other uses the terminal by watching our parents or friends a long time prior to our first time using it. This is knowledge a blind person doesn't have. We would know that we start by inserting our card and would know where to insert it by seeing the card slot. When inserted correctly the display changes and tell us to start typing the

PIN. A blind user would have to feel where to insert the card and when inserted the system does not provide any clue if it was correct and if the terminal was ready to receive the PIN code. The user would already have her PIN code for the card and as seeing the numeric pad with numbers we would associate the number on the keypad with the number in the PIN code. A blind user with knowledge on how a terminal is normally designed would start using her hands to locate the buttons. She might start by finding the buttons on the edges of the keypad and try to look for tactile markings. The five key in the middle is often (but not always) equipped with a tactile dot. If the dot is found she would know that the button on the left is a four and the one on the right is a six. If the keyboard uses phone layout where the top line of buttons from left to right is one, two and tree. A blind person would have to trust that the keyboard layout is like this and if a key pad would use the computer layout instead where the top line of buttons from left to right is seven, eight, nine it would be impossible to know what key to press except four, five and six even with a tactile dot on the five key. When typing the PIN code as seeing we use the text on the key and use eye and arm coordination and movement to find the right key before we press it. For a blind person she would have to use the mental picture of the keypad and move the hand to the right key. When pressed as seeing we can often see an start in the screen indicating that we have pressed the key. This signal is not received by a blind person. Some terminals uses a second modality in form of sound that indicate that the key is pressed. Sound modality will not work if the terminal is operated in a load environment like a pub with load music or a ATM located outdoor next to a busy street. When the PIN is entered the user have to locate the OK/Enter key, and as seeing we locate this with the text. The control keys often uses other modalities to inform the user like a tactile marking, colors, different size. From the model we see that some of the signals may be filtered out, like the color for color blind, text for dyslectic and so on. For a blind person locating the control key a terminal with many extra keys would be more difficult. If they would be located at the same place from terminal to terminal the blind user could use her mental picture of the terminal and start feeling in the area she would expect it to be.

From a security perspective a person trying to observe the entry of the PIN would have to see what key is actually pressed. The observer would do this by watching the fingers and see what key is pressed. Large keys can help as the hand movement would be more clear. Sound when pressing would help him understand when a key was actually be pressed. Observing a blind person that have to navigate to each key by feeling and the mental picture of the keypad is likely to take longer time than for a seeing and because of that give the observer more time to view the numbers that is pressed. Another problem for blind people are of course that they can not see if they are being observed and make counter measures.

In the next Chapter we will explain a new novel PIN entry method that may have some positive characteristics compared to the normal PIN entry method we just described and use the same model on that to see if the model can identify both benefits and security issues.

7 Using the evaluation model on a payment terminal with the new PIN entry method

7.1 New pin entry method

The new PIN entry method will not use the standard 0-9 keys that most payment terminals and ATMs use as input for typing the pin code when authenticating. Instead it uses two separate buttons, one for providing the number and one for moving to the next number. Figure 8 shows this new keypad. We call the two keys "Number" and "Next" from now on. To enter the pin with this method the user will have to press the "Number" key as many times as the pin number, then press the "Next" button to indicate the first number is entered. Then continue with the first key to indicate the second number and so on. The number zero will be entered with just pressing the next number key. If the pin is 1234 the user will press the "number" one time then the next key, "Number" key two times then the next key and so on. Figure 5 shows how this is done both with our method and what is normal today. If the pin is 2001, the user would have to press number key two times then the "Next" key tree times followed by the "Number" key one time and the "next" key. This is displayed in Figure 6.

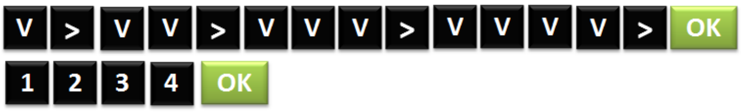


Figure 5: Displays how the PIN code 1234 is entered with the both new key entry and the normal way

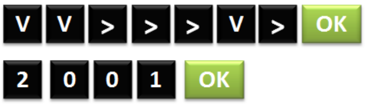


Figure 6: Displays how the PIN code 2001 is entered with the both new key entry and the normal way.

7.1.1 Possible benefits

We thought this method would have both positive and negative implications for usability, accessibility and security. Below we describe some of those. In the experiment we tried to measure these in a more quantitative way.

Usability

Since the method uses more of the cognitive skills where the user have to count the key presses inside his head he will be able to enter pin under different environments like darkness. The user should be able to feel the two keys with one hand and be able to enter the pin code under suboptimal conditions. The ’Number’ and ‘Next‘ key should be equipped with tactile markings making it easy to recognize them for people with visual disabilities.

Accessibility

For people with visual disabilities it should be easier to locate only two keys instead of the ten on a normal numeric keypad. It should be possible to enter the pin with only two or one finger.

Security

The benefit of this method should be that the entered pin should not be possible to be observed by other or by a video camera. Because the same button is used to enter all the numbers a third party observer only way of observing this would be to count the number of key presses and count them. The experiment will hopefully show that this counting is not possible or difficult.

7.2 Using the evaluation model

We will use the same evaluation model on the new PIN entry method. We only look at the two new buttons and the not the entire terminal and only add things that are new or different from an terminal with normal PIN entry. We start with describing the modalities used by our new PIN entry method. In Table 9 we list them with the effects they use. The new method is affected by the same effects because of disabilities as the old method 2. The difference from the old method comes from the hand movement effect witch is less than for a numeric key pad. Shape recognition should also be easier if the ‘Number‘ and ‘Next‘ keys is always found on the bottom part of the terminal. Both the buttons have tactile markings compared to the numeric key pad witch only have tactile markings on the five key.

Modality	Composed of	Effect which the modality use	Effect type
Keyboard	Number and Next keys	Hand movement	Motor
Keyboard	Number and Next keys	Pressure	Motor
Keyboard	Number and Next keys	Shape recognition	Perception
Keyboard	Number and Next keys	Tactile marking	Sensing

Table 9: Modalities and effects they use with new PIN entry method

In table 10 we list new security related incidents we could identify related to the new PIN entry method. The hand movement between each key press is less, but each button has to be pressed more times. If the hand movement between each key press is large the actual movement may be large also for the two key method. As the number of key presses on the number key is the same as the number in the PIN code sound from the buttons might make it easier for the observer to get the PIN code. Both sound created by the terminal and sound from the physical button might be used. On terminals with sound this can be turned off for these two keys to prevent the problem. The possibility to directly use the visual

If we try to imagine how an blind person would approach the new PIN entry method she would probably try to find the keys on lower edges of the keypad. The user would of course have to had the method explained and told where to locate the two new buttons. When the buttons is located the user may keep the fingers on the buttons during the PIN entry if she uses two fingers. If the user is using only one finger for both keys he would use the same skills as with the old

Modality	**Side channel**	**How**	**Risk**
Number and Next keys	Visual	Observer can see the hand movement and count number of presses.	Get the PIN code
Number and Next keys	Sound	Observer can by listening to sound from keys and count number of presses.	Get the PIN code
Number and Next keys	Movement	Observer can see the movement of the keys and count number of presses.	Get the PIN code

Table 10: Identified errors, mapped to error type and affected modality

method. The same apply to a seeing person. If he uses only two fingers hand/vision coordination is used to move between the keys. For each key press the user have to keep track of the count using his cognitive skills. As the user have to use his cognitive skills more the method may be more affected by user constraints like stress and social constraints like crowded areas. As long as the

The ‘Number‘ and ‘Next‘ keys are maybe more difficult to observe as the observer have to count and use both cognitive, sensing and perception to be able to observe the pin code. Sound from the keys may be easier to observe as we only have to distinguish between two keys. If we added sound to the ‘Number‘ key it would be much easier to count the number of presses only by using sound as observer able modality. When looking at it from a security perspective we can see that a solution that is usable for people with visual disabilities can probably also be used in darkness. Darkness on the other hand will make it much harder to do visual observation witch is the most common.

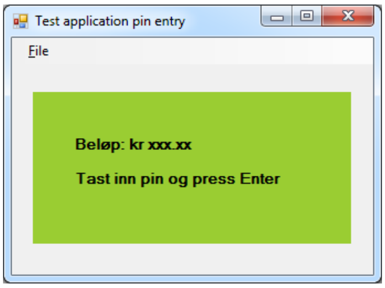
8 Experiment

8.1 Introduction

We want to test our novel new PIN entry method explained in Section 7.1 in a practical experiment on the usage of both that and the old PIN entry method. In this chapter we how we conducted the experiment on a group of users with visual disabilities and one with normal sight to see if the new method had the expected results.

8.2 Test application and prototype terminal.

An test prototype application was created to execute the experiment. In Figure 7 the simple windows application that mimic the pin entry procedure you find in most ATM's and payment terminals is displayed. A payment terminal most often consist of 4 rows and 3 columns of keys with some extra controls keys like "Ok", "Cancel" and "Abort". Since we have only 10 numbers the two last keys often placed at both sides of the zero key at the bottom is not used. In our PIN entry method we use these two keys as the alternative input method for the pin code. In Figure 8 our new key pad is displayed. We placed the control keys on the right side of the keypad.



Beløp: kr xxx.xx

Tast inn pin og press Enter

Figure 7: Application used in experiment.

In Figure 9 and Figure 10 examples of both ATM keyboards and payment terminals are displayed. On both of them you will see two keys on both sides of the zero (0) key that is not used in the normal PIN entry method where the pin is typed on the keypad. We would like our experiment to utilize these two keys as the 'Number' and 'Next' key. On the ATM keyboard in this example you see that they have added tactile clues on some of the keys. The 'OK', 'Correct' and 'Stop' button all have this plus the '5' key in the middle of the keypad. From our own experience this is not done everywhere and only some ATM keypads have this. On payment terminals it even more rare, but an indicator of the middle button '5' is often equipped with a dot. We used an down array as tactile marking for the 'Number' key and right arrow as the tactile marking for the 'Next' key. The symbol and tactile mark should tell the user what the key is used for and the arrows was what we thought would

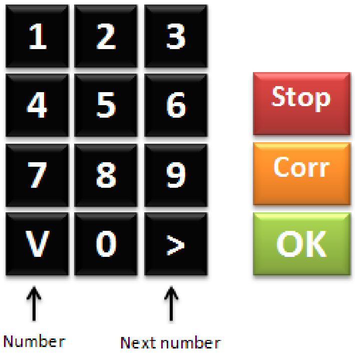


Figure 8: Keypad with the 'Number' and 'Next' keys on both sides of the zero key.

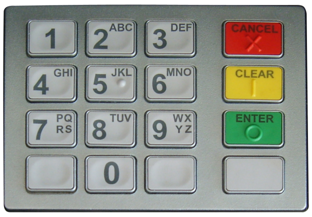


Figure 9: ATM keyboard layout displaying the unused keys besides the zero key.

We did not have access to a real payment terminal or ATM keyboard we used an external wireless keypad that we modified to mimic an payment terminal. In Figure 11 is a picture of the prototype. The keys on this is rearranged to be more like a normal payment terminal. Tactile cues with down and right arrow is added to support our experiment. Our prototype implements both the new and old PIN entry method in the same terminal.

The test application will mimic the behaviour you will find in most payment terminals where the amount you have to pay is displayed together with the information about what to do. For each pin entered a star (*) will be displayed. When 'Enter' is pressed the pin will be validated

Figure 10: Payment terminal layout displaying the unused keys besides the zero key.

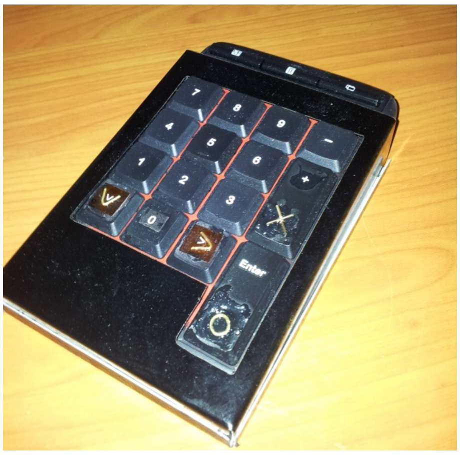


Figure 11: Picture of our prototype payment terminal keyboard.

and information to the user about the correctness or not will be displayed.

8.3 Measurements

The experiment had to test usability, accessibility and security. For usability we tested how easy it was to learn, understand and use the input method. Each participant in the experiment got the same explanation before the experiment started how the input method worked and how to use the application. We took notes about questions asked and if we have to explain the method multiple times. When the experiment started we measured the time the user uses to enter the pin with the new method. We also took notes of how many times the user entered the pin wrongly. All this was to test the usability. To test accessibility we took take notes if the two keys used for entering the pin is located easily by all the participants with and without disabilities. We also took notes if people used only one hand when entering the PIN-code. How many fingers they used, one, two or multiple. For security against shoulder surfing we used a video camera that filmed the hand to afterwards check if it was still possible to count the number of key presses to recreate the users pin code.

8.3.1 Usability

As we described usability in our problem description we will have to collect data on the following topics: Learnability, efficiency of use, memorability, few and non-catastrophic errors and subjective satisfaction. Some of these things are possible to measure quantitative and compare the old and new way against these. On the other hand subjective satisfaction is not possible to measure in the same way and we will use a qualitative method with an interview with each of the test persons to try to find out how they feel about the new input method. We will measure the time used to enter the pin with both the old method and new to measure the efficiency of use and memorability. The number of errors done when entering the pin will be used to test for learnability, memorability, few and non-catastrophic errors.

8.3.2 Universal design

To evaluate the universal design aspect and in particular improvements for visual impaired group of people we will use a qualitative approach. We interview the participants in the experiment both before they have tested our solution about their current experience with ATMs and payment terminals and also after they are done to get their immediate response of the usability. We will also use literature on universal design and different guidelines to help us understand how we may improve our solution to be easy to use for everyone. We will use one model in particular [32] where we can look at our PIN entry method when it comes to usability and accessibility together with the guidelines from the seven principles of Universal Design [15].

8.3.3 Security

Security or improved security by our solution will be evaluated by using a video camera to video tape all the participants usage of the prototype. We will use the videos to find out how easy it is to get the PIN code just by observing the PIN entry but also how easy it to afterwards use a video recording of it and by using slow motion, picture enlargement and other techniques find the PIN code. This will be done both on today's PIN entry method and our and we will try to compare if our solution is better than the old way. We will also extend the model from Obrenovic et. al [32] to include a security approach and use that model on our solution to see if new security vulnerabilities or improved security is added. We will also use models and ideas from safety planning to see if improvements or new security challenges arises.

8.4 Selection

We needed two groups of people to do our experiment, one with visual impairments and one without. Our group of people should be representative for the whole population, but as we have to get volunteers we would accept everyone that was willing to help us do the experiment. We contacted the association for visual impaired in the closest counties and sent them information about our project. They distributed this information to their members and they contacted us as they would like to participate. We also contacted one local county association to get more volunteers. Our final selection consisted of 6 people with different types of visual impairments ranging from completely blind to strong partially sightedness, four women and two men with an age ranging from 35 to 62 years of age. We selected the same amount of people for our test with people with no visual impairments with about the same age and gender diversity. In the second group we had seven people,

8.5 Design of prototype data collection and interview guide

Our prototype needed to collect information about how the user interacted with it. We collected the actual time the user used to enter the PIN code by taking the time difference from he started to type on the terminal to when the confirmation key was pressed. We also recorded if the correct pin was entered or not. A video camerae was set up and we videotaped the entire test session. The camera was placed so it mimicked the way a person would stand if he wanted to monitor the pin entry. Because of the location of the actual test the camera was sometimes placed on the right side and sometimes on the left side of the user. Sometimes it was possible to place it behind the shoulder of the user. The video will be used to see how easy it is to see what the user types on the keyboard. We made notes during the interview and created minutes from all the users after the experiment was finished.

8.6 Implementation of experiment and interviews

The actual interview and experiment was done by visited the participants at home as that was most convenient for the them. We also did some of the test at Gjøvik University Collage. A quick introduction about the project, motivation and general information about anonymity was given before we started the interview. The interview was done in a semi-structured way where we had a set of questions ready, but let the participants talk freely and only asked questions when there was something we did not get an answer to or wanted to clarify something. We tried to act as good listeners and act very polite to make the participants feel safe about the situation so they would talk more freely. Then we explained our new input method and if the participant wanted they could manually test the input method before the actual test was started. Most participants tried it one time before the actual test. Before the test was started we asked if it was ok to record the test with video camera and set up our video camera filming the prototype payment terminal and the users hand and started the experiment. During the test we observed the user and helped them if they had forgotten the correct pin code.

8.7 Collection of data for analysis

Collection of data for analysis had to be done in different ways. From our experiments we had data both in semi structured form from interviews, video of the participants interacting with the terminal and data collecting from the application during the experiment. The data from the application was easily transferred into and Excel data sheet for analysis. Both meta data about the participant together we timing of each pin code entry and number of errors was added per users.

The video of the experiments was analysed manually by watching the film one time and trying to observe each of the pin codes as the user typed them. Some of the tries was not possible to observe as the video starter too late to capture the first tries for some of the participants. We counted the number of observed tries and the number of tries where we was able to observe correctly the PIN code and added that to the Excel sheet together with the data from the application.

In the next chapter we use the developed evaluation model on the new PIN entry method to be able to compare it to the experiment data above, but also the differences with the old PIN entry method that we evaluated with the same model in 6.

9 Data analyse

Below we will analyse our research questions with the data we have collection through our evaluation method, experiment and interviews.

9.1 Usability

9.1.1 Learnability

Each of the test persons got a brief description of the PIN entry method as described in the interview guide. Before we started they also got the opportunity to test the new PIN entry method before we started the actual test. To evaluate the learnability we use what the users said after they finished the test. Some of the users did do the test and needed an extra explanation before the actual experiment started. There were in particular questions about zero and how to finish one number and go to the next. Most of the user expressed after the test that the new PIN entry method was easy to learn, but some expressed that it was new and unfamiliar. One blind test subject with no previous experience with using payment terminals and ATM today had an error rate of 50% with both PIN entry methods. Our method had more errors among people with visual disabilities than people without, but this was not reflected in the answers they gave after the test was finished.

Our conclusion for learnability is that the new PIN entry method is easy to learn and understand.

9.1.2 Efficiency of use

The actual time spent on the PIN entry was measured by taking the time from the user started to type on the keypad to the enter key was pressed. Included in these numbers are also the time it took when they typed the wrong pin code, and when they first typed the wrong PIN code and then cancelled and corrected it. Each subject typed the same password tree times. We did not use the first occurrence in our measurement in case there was a high learning curve. To have comparable numbers we also used the measurements where everyone used the same PIN code.

On average people used 5.4s with the old method and 19,5s with our method. For the group of seeing the average was 2,8s with the old method and 14,6s with our method. In the group with visual impairments the average was 10,3s with the old method and 28,1s with out method. From studies [9] of real world usage the PIN entry takes about 2s. For our group of seeing subjects we have slightly higher than this, but for everyone the average is much higher. The fastest time for normal PIN entry used by everyone was 1,54 second and the highest time was 32,2s. Why we had such large differences on the known old method could be because one of our visual impaired users was not used to using ATMs and payment terminals at all. Our relatively small amount of participant makes a big difference with values that differs a lot from the others. For our method the fastest time was 7,34s and the slowest 53,7s. The same subject used in this method much longer time than the others. To compensate for these extreme values a better measure could be to use the median times. The mean time for the old method for all subjects was 2,61s and for our method 15,87s. 2,61s correlate better with what was reported as normal time for PIN code entry in [9]. Table 11 and Table 12 show a summary of measures of time used.

	Average	Median	Min	Max
Visual impairments	10.33s	3.24s	1.9s	32.23s
No visual impairments	2.8s	2.54s	1.54s	5.6s
All	5.43s	2.61s	1.54s	32.23s

Table 11: Measurements old PIN entry method

	Average	Median	Min	Max
Visual impairments	28.06s	20.43s	7.34s	53.73s
No visual impairments	14.64s	13.34s	7.62s	26.24s
All	19.52s	15.87s	7.34s	53.73s

Table 12: Measurements new PIN entry method

From the numbers above it's quite clear that our method is slower than the normal way, but that was to be expected as the input method requires more key presses especially with large numbers in the PIN code. In the common PIN code everyone types and we did our measurements was 9067. With our method it required 24 key presses compared to 4 with the old method.

The median time used with the new method was 15,9 seconds and 2,61s seconds with the old. This is quite large difference, but as many of the participants told they felt the method was unfamiliar and thought that by practice they would do it faster.

Our conclusion for efficiency of use is that it is much slower than the normal way, but this time may go down as people get used to using it.

9.1.3 Memorability of the method

Since we only did one experiment with each person it's difficult to say much about how easy the method is to remember after they have learned it, but we choose to use the same information as we used with the learnability. Why we had such high numbers of errors may have to do with people finding it difficult to memorize two new PIN codes and not how to remember how to use the input method.

9.1.4 Few and non-catastrophic errors

We counted the number of times the user typed a wrong pin with both new and old method. In total we had eight errors with old method and ten with the new method. We recorded a total of 78 test with the old pin and 78 tests with the new method. Our method had slightly more errors than the normal method, but no statistical difference. A T-Test gave $P - Value = 1$. Table 14 and Table 14 details about errors done are listed. Figure 12 and Figure 13 displays a graphical representation of the errors done among all users. Figure 14 to 17 show the percentage among the two test groups. The number of errors is quite large and we will discuss this further in the next chapter.

	Number of tests	Number of errors	Percentage of errors
Visual impairments	36	3	8%
No visual impairments	42	5	12%
All	78	8	10%

Table 13: Errors old PIN entry method

	Number of tests	Number of errors	Percentage of errors
Visual impairments	36	6	17%
No visual impairments	42	4	10%
All	78	10	13%

Table 14: Errors new PIN entry method

9.1.5 Subjective satisfaction

We used the information from the interviews after the test was finished where we asked them about their immediate reaction to the new PIN entry method. Only one of the users was sceptic to the solution and liked the old method better. Most of the users found the new method unfamiliar, but thought it would be easier if they used it regularly. Some complained that they had to be much more focused as they had to keep the count in their head, but others said that this was actually a good thing as they got more focused. Most of the blind subjects like that it was easy to locate only two buttons compared to ten with the normal method.

9.2 Universal design

9.2.1 Equitable Use

This design principle states that the design should be marketable to people with diverse abilities. We have tested our PIN entry method on two different groups, both of the groups found the solution easy, but unfamiliar. Most of the visual impaired users found it easy to navigate to only two buttons instead of the normal 0-9 buttons. This was not the case for the other group as they all was used to using their eyes to locate the buttons. The guideline also suggest that the system should provide privacy, security and safety for all users. For our two groups of test persons our prototype support this principle.

9.2.2 Flexibility in Use

This principle states that the design should provide choice of method. Our prototype supports both the new and old PIN entry method. We choose to use two buttons not commonly used making it easier to implement on already existing equipment and at the same time support the old PIN entry method. In our experiment only one of the PIN entry methods worked at the same time, but it should be possible to let the user just select the method he/she is preferring to use. We tested both left and right handed users and none of them mention that it was more difficult with either way. The guidelines also states that the design should provide adaptability to the user pace. Our PIN entry method does not time out and the user can use as long time as he feels like. They way our prototype is implemented with the support of both old and new PIN entry method this principle is satisfied.

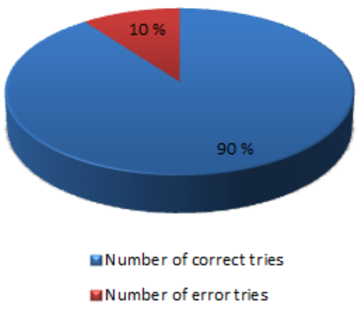


Figure 12: Percentage of errors with old PIN entry method.

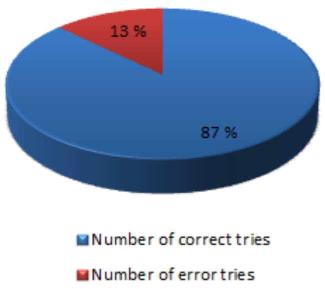


Figure 13: Percentage of errors with new PIN entry method.

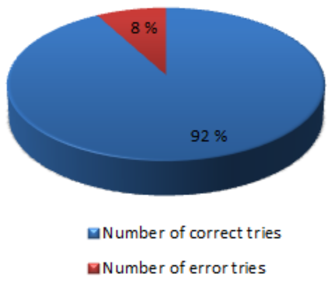


Figure 14: Percentage of errors with old PIN entry method among blind test persons.

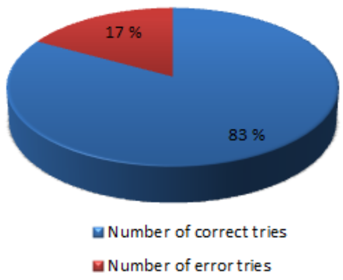


Figure 15: Percentage of errors with new PIN entry method among blind test persons.

9.2.3 Simple and Intuitive Use

This principle is about usability and we answered that in our part on usability. The last guideline suggests that the solution should provide effective prompting and feedback during and after task completion. Our prototype did only provide visual feedback during the PIN entry in the form of stars (*) for each entered number. Not all, but most ATMs and payment terminals do provide a sound when buttons are pressed. We can't use this in our PIN entry method as this would make it easier to count the number of key presses. We will further discuss this in the next chapter. Some of the visual impaired users mentioned that one of their biggest challenges with payment terminals in general was to know when they should could start entering the pin as this was only given through what was written on the screen. Our PIN entry method does not improve this problem, but as both user groups found the PIN entry method easy we think we support this principle. More work could be done to improve the prompting and feedback without sacrificing security.

9.2.4 Perceptible Information

How does the design communicate necessary information effectively to the user, regardless of ambient conditions or the user's sensory abilities? We added tactile markings on both of the keys

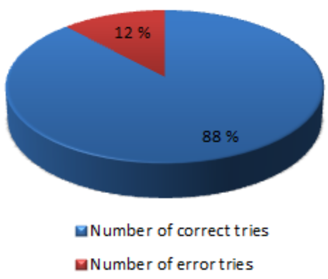


Figure 16: Percentage of errors with old PIN entry method among seeing test persons.

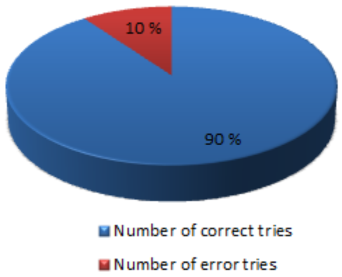


Figure 17: Percentage of errors with new PIN entry method among seeing test persons.

used in our prototype. The markings were formed as a down arrow for the key to enter the number and a left array for the next number key. None of the keys in between or above our keys had tactile markings so they were easy to find for the group with visual disabilities. By only having two keys instead of ten for the old PIN entry method our PIN entry method supports this principle. To make it even easier the keys could have had different colours and form than the rest of the keys.

9.2.5 Tolerance for Error

Authentication with PIN codes and passwords does not provide the possibility to be half right or half wrong. The PIN code has to be entered 100% correctly or it will not authorize correctly. The solution should on the other hand have the possibility to cancel or correct errors if the user notices an error. Our prototype used the same options as most payment terminals offers. A correct/cancel button is available that let the part of the pin code already entered be cancelled so they could start over and a abort button. In the experiment users who did mistakes and wanted to cancel spent quite some time to locate before they pressed this button. Some of our test persons felt that we maybe should have the possibility to only cancel the current number they were typing and not having to cancel the entire PIN and start over.

9.2.6 Low Physical Effort

Not much physical effort have to be used in any of the PIN entry methods with our terminal. With our PIN entry method the user only have to press two buttons, but they have to be pressed more times than the old PIN entry method. With our PIN entry method the hand movement and the location of the keys is less, but as you have to do more presses a person with motor constriction may have problem with it or find it difficult to press the keys the right number of times. Our PIN entry method does support this principle just as the old PIN entry method does.

9.3 Security

9.3.1 Shoulder surfing

We wanted to test if our new PIN entry method was more resilient to observation attacks like shoulder surfing. We watched the videos from the experiments and counted the number of PIN codes we could identify by observing both with the new and old method. In our experiment we were able to observe 63% of the tries with the old method and 51% of the tries with our new method. Figure 18 and Figure 19 shows charts of the results.

When performing a T-Test over the dataset of observation we get a $P{-}Value = 0,36$ indicating that there is no statistical difference between the observation of the new and old PIN entry method.

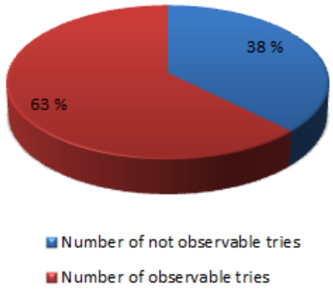


Figure 18: Percentage of PIN code observation old method.

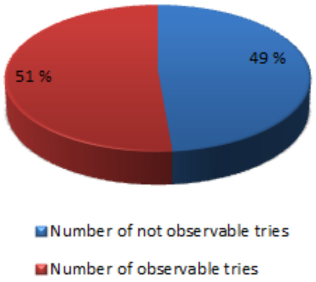


Figure 19: Percentage of PIN code observation new method.

Many different factors influenced how easy it was to observe the pin entry. The placement of the camera on the left of right side made a big difference if the user was left or right handed. If the camera was placed behind the left shoulder and the subject was left handed it was much harder to observe both the new and old method. And if the user was right handed and the camera was placed behind the right shoulder and the subject was right handed it was the same. None of the test subjects used the second hand to cover the input. From the interviews only 7 of the 13 test subjects said they normally did this, but some of them mention that they only did it when they remembered to do it. How many fingers and the typing speed also influenced how easy it was to observe. Subjects using multiple fingers on one hand was hardest to observe with the old method. Typing speed and how large the movement of the fingers influenced the observation of our method. Some subjects used only one finger, typing very slow and huge movement making the observation easy. For the our new method the problem was mostly that you get out of count of the number of key presses on the ‘Number‘ key. You often missed one key press or counted one to many. Zero in the PIN code was also hard to observe especially if the subject pressed the "Next" key fast.

9.4 Summary of the analyses

Our PIN entry method is worse than the normal way in both the time used and number of errors. The median time used with the old method was 2,61s and with our method 15,87s. People without visual disabilities used slightly less time with both PIN entry methods. The fastest time with our PIN entry method was done by a blind person with a PIN entry time of 7,34s. Our solution is simple to learn and the subjective satisfaction from out test persons is good. We will discuss some of the factors that can influence this in the next chapter.

Our prototype supports most of the principles from universal design, but further improvements can be done to make it even better.

From our analysis it looks like the new PIN entry method is slightly better than the old method, but it's not completely resilient to observation attacks as we hoped.

10 Discussion

In the following chapter we will further describe our research questions and discuss our assumptions, results and our research model in more detail. We will also say something about how our approach to this experiment went and what may have been done different. In the end we will give some general recommendations to vendors and financial institutions responsible for the design of ATMs and payment terminals.

If we look back at our research questions we wanted to look at how we could design an authentication solution where we made use of principles from universal design. We further wanted to test if our new PIN entry method was a method that could replace the way we do it today. To do that it had to have some benefits. We used our evaluation method on an payment terminal with the normal PIN entry method and used the same model on our new PIN entry method. We conducted and experiment to get practical feedback on the methods where we looked at three main areas. Did our method have better usability than the old method? Did our method support more principles from universal design making it easier or more accessible to more people and in the last question we wanted to test if our method would solve one of the remaining security issues with credit card scams witch is shoulder surfing.

10.1 Discussion of our new evaluation model

We used the evaluation model on an payment terminal both with the normal keypad and the two button input. When looking closely on how a user might approach a system and look at what modalities and what human skills is used to find, understand and operate different elements of the user interface the model is a helpful tool. Not focusing on a disability as something negative, but one of multiple constrictions to the usage makes the model a good choice. As with all public access terminals that have to be usable in a lot of different scenarios we can't use it to drill really close to a particular situation that would have more restriction and effects on the usage. The need for simple and intuitive user interfaces becomes clear and by using it is clear that extra buttons not used in the normal operation makes the usage more difficult for visual disabled people. Adding security in the form of observation attacks to the model and see how the same constrictions apply to the observation in the same way as the usage is helpful. Functionality that an blind user can operate easily could also be operated by everyone else without the need of visual effects like in darkness. When not relying on vision the functionality could be totally shielded from observation by covering the input. Today some payment terminals have plastic covers around the keypad. With our two key PIN entry method this cover could for instance be created so the hand entering the PIN code is totally covered by the plastic cover. This would make observation attacks using vision impossible.

10.2 Discussion of our new PIN entry method

Below we describe each of the variables related to usability, universal design and security.

10.2.1 Usability

We concluded in our analyses that the usability of our method was worse than the old method because it took much longer time to enter the PIN code with our method compared to the old way. Many of our test persons told that the method was new and unfamiliar. We probably use longer time with something we are unfamiliar with and that could explain some of the difference. We would probably see an improvement in time spent as people got more familiar with our method, but how much it would improve is not easy to say. It would probably never be as fast as the old way as the number of key presses is higher even when the numbers in the PIN code is small. Our method also had slightly more errors than the old method. The difference was so small that we cannot conclude that because of this it is more difficult to use. Why the number of errors was so large for the old method is maybe surprising. How often people do errors today when using payment terminals is not something we have data on. As with typing speed the number of errors may go down as people get more familiar with the method. Both the speed of typing and number of errors may also be affected by the PIN code they used and the one selected by us. The one selected by us was chosen to include both large numbers and zero. The feedback from the user after the test was that large numbers was harder to use than small and some found the notion of entering zero a bit confusing in the beginning. Usability is also about how easy it is how to remember how to use it. As we tested each subject only one time, we cannot conclude based on the number of errors that people would remember it the next time they use it. On the other hand if this method is implemented and people use it daily we would guess that people won't have to remember it from time to time. The method was well received by most of the test persons. One of the test persons without visual disabilities told that he was dyslectic and that he usually remembered the password by remembering the pattern the key pad his normal PIN formed. He liked the method as he had to be more focused and it would probably also help him in remembering the password. Another of our test persons told us that he just prior to the test had to take migraine medicine and that his concentration was affected by this. This test person did not do any error with the new method, but did with the old way. One of our testers just had here first credit card six months ago and was not as used to using the old method as many of the others. She also found it unfamiliar, but found it easy to learn and use. One of the blind users was not used to using either ATMs or payment terminals and he did the same amount of errors on both methods. One weakness in our experiment approach was that we conducted the experiment and interview personally. Even when we told the participants to be honest with the feedback is that they might be hesitant to tell us any negative as we were present. Maybe if the feedback would be presented anonymously in a questionnaire people would have been more open about weaknesses with the design.

One possible reason we saw high number of errors both in our method and the old way may be because the user did not remember the chosen PIN code. The test application both displayed the PIN code on the screen and we used speech synthesis to say the PIN code before it should be written. Still remembering two four digit PIN codes seemed difficult for some of our test persons.

With a PIN code you use multiple times a day we would probably see less errors because the user will remember it easily.

Comparing the usability of our solution to other research on shoulder surfing defence [35] [36] they operated with an acceptable authentication time of 60s. Our tests shows that our PIN entry method in most cases is faster than this.

10.2.2 Universal design

We evaluated our solutions based on the principle and guidelines from The Center of Universal Design [15]. Multimodality seems to be a principle that many emphasize on when it comes to universal design [17] [39] [32]. The simplicity of our solution made it easy to support both the existing method together with ours, making it multimodal. Most of the visual impaired users liked the fact that they only had to locate and use two buttons instead of ten. One problem with our solution is that it does not directly tell the user what to do. With a number pad with numbers corresponding to the number in the PIN code as we have today it is probably obvious to most users that they should press the number corresponding to the number in their PIN code. With our solution there is probably a higher need of explanation and training. We provided our button with a down array and a right arrow. Maybe another sign could make it more obvious what the buttons was used for. The arrows were made tactile as well to make it more recognizable for visual impaired users. Another problem with our solution is that it does not give good feedback during the entry of each number. It does not provide the user with information about how many key presses they have done so far and if the user gets out of track of the counting the system is not providing her with any feedback. The keys did not provide any feedback that they were actually pressed in a form of a sound or other feedback. We will come back to our reason for this when we discuss security, but from a universal design perspective this is a drawback.

One interesting thing that was brought up with some of the visual impaired test subjects was how they used signals from existing equipment that probably was not part of the designers intention to solve some of their problems. Some of them mention the problem with knowing when to start typing the PIN code as a problem as the ATM and terminal did not inform them in any way except on the screen that they should start typing the PIN. One subject was using the fact that some payment terminals right before they was about to abort the transaction because they had not received any input started to making a sound. If she waited for this sound she knew it was ready for input of the PIN code. Another subject used the sound from the card reader, money dispenser and receipt printer to know where in the process she was when using ATMs.

One quite surprising comment given by many of the subjects with visual disabilities was about ATMs with extra sound menus made especially to support this group of people. Even if they new some ATMs had this feature they did not use it. Different reason was given, but some mention that they did not bring there own head phones. Some told they felt they lost their orientation about the surroundings. The number of ATMs with this feature was also a problem as some lived in cities where no ATM had this feature.

10.2.3 Security

The third variable we studied was if our method would show improvements to the security challenge with observation attacks and in particular shoulder surfing. In the analysis we could see an small improvement. We where able to observe 63% of the pin entries with the old method and 51% with our new method. Our method is not completely resilient to such attacks. When setting up the experiment we only used one camera that we placed on a tripod behind the user. The camera was put on the left and right side depending on the location and where it was place able. We noticed when looking at the recordings that if the camera was placed behind the right or left shoulder and if the user was right or left handed made a big difference in the probability of observing the PIN code both with our method and the old way. If the user was right handed placing the camera on the left side made it easier and for left handed people placing the camera on the right side would be easier. The reason for this is that the fingers are partly covered with the palm of the hand if the camera is placed on the correct side. Using two cameras on both sides would probably have given a higher percentage of observations of both methods. Covering the PIN entry with our other hand or with our wallet is one recommendation that the credit card companies and banks tell us to do. During our experiments none of our test persons did this. During the interviews some of them said they did this only if they felt they were being observed. Some told that they did not bother covering it at all and some tried to cover the entry by using their upper body to lean over the terminal. The fact that the users felt safe because it was an experiment done in a setting making the users more safe may also have affected how they typed and why none of them did anything to cover the PIN entry. One thing we learned from the videos is that how people type is very different. It sounds like a trivial task to type the PIN, but when humans are involved the way they used their hand and typed was very different. Some used two hands and two fingers, some used one hand with two fingers, others used one hand with one finger and some used one hand with all their fingers. The speed of the typing was also very different. This made the observation different from person to person. People using one hand with all their fingers was clearly more difficult to observe than people using only one hand with only one finger typing very slow. Visual impaired and in particular the test persons with no sight at all were using all of their fingers and was hard to observe. This may be because they can't use the vision to locate anything and have to trust what they feel with their fingers. For this group of users the observation was more difficult. One possible weakness in our analysis is that we who was part of the experiment and conducted the interview also were the persons that analyses the videos. The number of participants was so low that just by watching the hand and table we would sometimes know who the test person was. We also knew the common PIN code selected by us in the application and it may have been easier to observe this PIN code for us than it would have been for a person not knowing it. We had this knowledge for both the old and new PIN entry method, so it affected the observation of both the methods equally.

From our evaluation model we saw that sound if added to our button presses would make it easier to observe the PIN code. Not only sound added by the system, but the actual sound from the button when pressed would help the observer count the number of key presses and in that way get the PIN code.

Another problem with our method is that the time it takes to type the PIN code is different between different PIN codes. If users where able to select their own codes, they may start selecting PIN codes that made the typing time less to save time. This could reduce the security as the number of PIN codes in use would be less. If users type the PIN with the same speed it could be possible to guesstimate the entered pin by the total time the user used.

10.3 Research method review

In the following chapter we will say something about our research method and design, data collection and something about reliability and validity of our thesis results.

10.3.1 Research design

We used both quantitative and qualitative methods in our research. We did use a qualitative design as the selection of people from the visual impaired group is limited and we wanted to test the prototype early to get an indication if the idea was something to go forward with. The interview guide could maybe have more detailed questions to better codify it afterwards. Our experiment application let us collect data from the experiment that could easily be used in a qualitative way. To get results with fewer possibilities for errors our amount of data should be higher.

10.3.2 Data collecting

Our selecting of participants for the experiment was not completely random as we had to use persons that were willing to participate. We interviewed and tested 6 persons with visual disabilities, five female and one male ranging from the age 35 to 62. We contacted tree offices of the visual blind organization in Norway asking for volunteers. If these persons represent the group of as a whole cannot be verified. The other group of test persons was selected to have about the same age range and gender distribution. We tested 7 persons in this group, 4 females and 2 males ranging from age 14 to 59. We added one test subject who just recently had started using a bank / credit card with the age 14. The video filming was done a bit different from test to test as the camera tripod had to be place able, but we tried to locate it in the same position mimicking a person looking over the left or right shoulder.

10.3.3 Data analysis

Validity and reliability tell us to witch degree we may have errors in our measurements [33]. Reliability is related to in with a similar study would yield the same results and validity is about if our results is correct or not. If similar studies give the same results we have high reliability. We have tried to be objective and critically review the collected information so that the results can be viewed in an scientific way.

11 Conclusion

11.1 Main problem and limitations

In this thesis we wanted to look at how we could use principles from universal design when designing authentication solutions and at the same time solve security challenges. We created a theoretical evaluation model explained in Chapter 5 that we used on today's payment terminals PIN entry method. We also wanted to evaluate a new idea for an authentication procedure for PIN entry shown in Section 7.1. The idea for the PIN entry method was that it should be easier for visual impaired users to operate and at the same time be useful for everyone. The PIN entry method was evaluated with principles from universal design and usability. We also hoped that the PIN entry method would show improvements over the normal PIN entry method to a specific security challenge, shoulder surfing attacks. We used the same evaluation model on our new PIN entry method. We also wanted to test our idea in practice and conducted a experiment on it to compare it to what our model showed. Our new PIN entry method was evaluated against the tree variables, usability, universal design and security. We did not get enough subjects with visual impairments to evaluate the variables statistically. We therefore used interviews together with the experiment where both old and new input method was tested. The experiment was done with test users with and without visual disabilities. We used data from the interviews and experiment together with our theoretical model to evaluate our PIN entry method.

11.2 Summary of our most important findings

Using the evaluation model on authentication solutions was a good way of doing the design process. For designers to think about what kind of human skills is needed when operating different parts of the system gives them valuable information. To see what constrictions not only related to a persons disability, but other factors influence the interaction. The extension to the model where it also included security related to observation attacks helps with understanding what signals exchanged between the user and system that can be intercepted. How different constrictions influence both the usage and observation can help in designing better solutions. Shoulder surfing of PIN entry rely on vision to be successfully. Designing solutions that can be used by people with visual disabilities also mean they most likely can be operated by not relying on vision for everyone else. Such a solution would for instance be possible to operate in complete darkness or somehow totally covered for observation. The model focus on disabilities as just another constraint instead of just disregard an idea if you it does not work for a particular handicap.

The PIN entry method was well received by our test subjects with and without visual impairments. They found it unfamiliar, but that was to be expected, but at the same time none said anything about it was difficult to learn or use. The visual impaired users liked that the method only used two keys as it was easy to locate them. The method requires people to use their cognitive skills more as they had to be concentrated and count each number in their own mind. The method was significantly slower than the method we use today. This was not a surprise either as most subjects is familiar with the normal way of entering PIN codes and new to the new method at the same time our method requires more key presses and the number of key presses increases when the PIN code consists of high numbers.

We found that our PIN entry method did not provide very good protection against shoulder surfing. It showed a small improvement compared to the regular way, but not as high as we hoped. As the subjects said, they had to be more focused and concentrated also applied to the person trying to observe the PIN entry. The higher numbers was harder to observe than the low ones. What we found through our study was than even what we think is a very simple procedure is executed very differently by different people. This is something that really needs to be taken into consideration early when designing new solutions where people are involved.

As history have showed earlier [42] designing with universal design and challenges for people with disabilities can improve our everyday usage of systems. Our PIN entry method was well received by the users, but did not show major improvements when it came to shoulder surfing attacks. Our method was simpler and did not rely on new hardware and still showed comparable results when it came to usability as other method that was tested against shoulder surfing. Our PIN entry method can also be implemented on many existing terminals and ATMs as we rely on keys that in most cases is not used. The evaluation model is useful to really understand how the usability is affected by different constrictions.

11.3 Further research

Our PIN entry method was only tested on a few subjects and in a controlled experiment settings. Public access terminals are operated in many different settings where people are in different emotional, social and user states. The method should be tested in more real life scenarios and with a bigger group of people. It should also be tested by the same people over a longer time period to see if the typing speed and error rate would go down. Our method because it uses more cognitive skills as the user has to count inside his head should also be tested for memorably. For instance is it know that people remember things more easily if more cognitive skills is involved [18]. Our evaluation method could also be used on other authentication scenarios to see if it would reveal both new benefits and new security challenges. Our PIN entry method does not relay on vision to be operated if the keys are easy to locate. One improvement that should be tested is if it could for instance be placed inside a box where the user puts his/her fingers inside. That way no observation could be done. Sound from the buttons is still a problem and further research on how to prevent this would have to be done. We haven’t found any information on why the terminals is equipped with extra unused buttons and why the keys are placed on different locations. Why vendors create these devices with different designs is also something that should be investigated.

Bibliography

[1] Iso 9241-11 ergonomic requirements for office work with visual display terminals (vdts) part 11: Guidance on usability. iso., 1998.

[2] Anne Adams and Martina Angela Sasse. Users are not the enemy. *Commun. ACM*, 42:40–46, December 1999.

[3] Aftenposten. Blir ikke trodd av dnb nor. `www.aftenposten.no/okonomi/innland/Blir-ikke-trodd-av-DnB-NOR-5317185.html`, Februray 2010 (Visited 4.3.2012).

[4] Frank Robert Berg. Finanstilsynets risiko- og sårbarhetsanalyse 2010. `www.finanstilsynet.no/Global/Venstremeny/Foredrag_vedlegg/2011/ROS_rapporten_2010.pdf`, Mars 2011 (Visited 30.5.2012).

[5] Nigel Bevan. Ux , usability and iso standards. *CHI 2008 Workshop on User Experience Evaluation Methods in Product Development*, pages 1–5, 2008.

[6] Sacha Brostoff and M. Angela Sasse. Safe and sound: a safety-critical approach to security. In *Proceedings of the 2001 workshop on New security paradigms*, NSPW '01, pages 41–50, New York, NY, USA, 2001. ACM.

[7] John M. Carrol, editor. *Hci models, theories and frameworks Towards a multidisciplinary science*. Morga, 2003.

[8] Alan Cooper. *The Inmates Are Running the Asylum*. Macmillan Publishing Co., Inc., Indianapolis, IN, USA, 1999.

[9] Alexander De Luca, Marc Langheinrich, and Heinrich Hussmann. Towards understanding atm security: a field study of real world atm use. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, SOUPS '10, pages 16:1–16:10, New York, NY, USA, 2010. ACM.

[10] Alexander De Luca, Emanuel von Zezschwitz, and Heinrich Hussmann. Vibrapass: secure authentication based on shared lies. In *Proceedings of the 27th international conference on Human factors in computing systems*, CHI '09, pages 913–916, New York, NY, USA, 2009. ACM.

[11] Sidney Dekker. *The Field Guide to Understanding Human Error*. Ashgate Publishing Company, Brookfield, VT, USA, 2006.

[12] European Telecommunications Standards Institute (ETSI). Etsi tc tr 007 human factors (hf); user requirements of enhanced terminals for public use. `www.etsi.org`, 1996.

[13] Finansnæringens Fellesorganisasjon. Kortsvindelen går ned. `www.fno.no/no/Hoved/Aktuelt/Pressemeldinger/2012/Kortsvindelen-gar-ned/`, April 2012 (Visited: 10.4.2012).

[14] P. M. Fitts. The information capacity of the human motor system in controlling the amplitude of movement. *J Exp Psychol*, 47(6):381–391, June 1954.

[15] Center for Universal Design. The principles of universal design. `www.ncsu.edu/project/design-projects/udi/center-for-universal-design/the-principles-of-universal-design/`, May 2011 (Visited 4.5.2012).

[16] K. Fuglerud and O. Dale. Secure and inclusive authentication with a talking mobile one-time-password client. *Security Privacy, IEEE*, 9(2):27 –34, march-april 2011.

[17] Kristin S. Fuglerud. Inkluderende identitetshåndtering. NorSIS security divas, January 2012.

[18] Lorrie Faith & Simson Garfinkel, editor. *Security and Usability Designing secure systems that people can use.* O'Reilly Media, Inc, 2005.

[19] Anja Tho Gunnersen. Frykter stoerre pågang av skimmere til norge. `www.tv2.no/nyheter/innenriks/krim/frykter-stoerre-paagang-av-skimmere-til-norge-3326009.html`, Oktober 2010 (Visited 4.2.2012).

[20] International Telecommunications Union (ITU). Itu e135 human factors aspects of public telecommunications terminals for people with disabilities. `www.itu.int/`, 1995 (Visited 12.4.2012).

[21] Einar Snekkenes Kirsi Helkala. Formalizing the ranking of authentication products. *Information Managment & Computer Security - Special Issue*, 17:30–43, 2009.

[22] Lothar Fritsch ï¿½ystein Dale Kristin Skeide Fuglerud, Arthur Reinertsen. Universell utforming av ikt-baserte løesninger for registrering og autentisering., January 2009.

[23] 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, pages 289–290, New York, NY, USA, 2010. ACM.

[24] Manu Kumar, Tal Garfinkel, Dan Boneh, and Terry Winograd. Reducing shoulder-surfing by using gaze-based password entry. In *Proceedings of the 3rd symposium on Usable privacy and security*, SOUPS '07, pages 13–19, New York, NY, USA, 2007. ACM.

[25] Pat Langley. User modeling in adaptive interfaces. In *Proceedings of the seventh international conference on User modeling*, UM '99, pages 357–370, Secaucus, NJ, USA, 1999. Springer-Verlag New York, Inc.

[26] Barne likestillings-og inkluderingsdepartementet. Lov 2008-06-20 nr 42: Lov om forbud mot diskriminering på grunn av nedsatt funksjonsevne (diskriminerings- og tilgjengelighetsloven). `www.lovdata.no/all/hl-20080620-042.html`, June 2006.

[27] I. Scott MacKenzie. Fitts' law as a research and design tool in human-computer interaction. *Hum.-Comput. Interact.*, 7(1):91–139, March 1992.

[28] Sindre Granly Meldalen. Her blir hun plyndret. www.dagbladet.no/2009/12/07/nyheter/innenriks/tyveri/organisert_kriminalitet/9391789/, December 2009 (Visited 4.3.2012).

[29] United Nations. Convention on the rights of persons with disabilities. www.un.org/esa/socdev/enable/rights/convtexte.htm, December 2006 (Visited 1.5.2012).

[30] Jakob Nielsen. *Usability Engineering*. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 1993.

[31] Z. Obrenovic, D. Starcevic, and B. Selic. A model-driven approach to content repurposing. *Multimedia, IEEE*, 11(1):62 – 71, jan.-march 2004.

[32] Zeljko Obrenovic, Julio Abascal, and Dusan Starcevic. Universal accessibility as a multimodal design issue. *Commun. ACM*, 50:83–88, May 2007.

[33] Jeanne Ellis Ormrod Paul D. Leedy. *Practical Research: Planning and Design (8th Edition)*. Prentice Hall, 8th edition, 2004.

[34] J.T. Reason. *Human Error*. Cambridge University Press, 1990.

[35] Volker Roth, Kai Richter, and Rene Freidinger. A pin-entry method resilient against shoulder surfing. In *Proceedings of the 11th ACM conference on Computer and communications security*, CCS '04, pages 236–245, New York, NY, USA, 2004. ACM.

[36] Hirokazu Sasamoto, Nicolas Christin, and Eiji Hayashi. Undercover: authentication usable in front of prying eyes. In *Proceedings of the twenty-sixth annual SIGCHI conference on Human factors in computing systems*, CHI '08, pages 183–192, New York, NY, USA, 2008. ACM.

[37] M. A. Sasse, S. Brostoff, and D. Weirich. Transforming the 'weakest link' a human/computer interaction approach to usable and effective security. *BT Technology Journal*, 19:122–131, July 2001.

[38] Nitesh Saxena and James H. Watt. Authentication technologies for the blind or visually impaired. In *Proceedings of the 4th USENIX conference on Hot topics in security*, HotSec'09, pages 7–7, Berkeley, CA, USA, 2009. USENIX Association.

[39] Constantine Stephanidis. *The Universal Access Handbook*. CRC Press, Inc., Boca Raton, FL, USA, 1st edition, 2009.

[40] Digital Accessibility Team. Public access terminals standards. http://www.tiresias.org/research/standards/pats.htm, November 2009 (Visited 12.4.2012).

[41] Finn Erik Robstad TV2. Lommetyvbande herjer i oslo. www.tv2.no/nyheter/innenriks/krim/lommetyvbande-herjer-i-oslo-3741325.html, Mars 2012 (Visited 1.4.2012).

[42] Tom Vavik, editor. *Inclusive buildings, products & services Challenges in universal design*. Tapir Academic Press, 2009.

[43] Susan Wiedenbeck, Jim Waters, Leonardo Sobrado, and Jean-Camille Birget. Design and evaluation of a shoulder-surfing resistant graphical password scheme. In *Proceedings of the working conference on Advanced visual interfaces*, AVI '06, pages 177–184, New York, NY, USA, 2006. ACM.

[44] Nur Haryani Zakaria, David Griffiths, Sacha Brostoff, and Jeff Yan. Shoulder surfing defence for recall-based graphical passwords. In *Proceedings of the Seventh Symposium on Usable Privacy and Security*, SOUPS '11, pages 6:1–6:12, New York, NY, USA, 2011. ACM.

12 Appendix A Interview guide

12.1 Introduction

Tell them a short introduction about myself and my motivation to do this master thesis.

- Frustration with ATMs and payment terminals lack of consistence when it comes to user interface for me without any disabilities.
- My sisters being shoulder surfed and credit card stolen at Gardermoen.
- Universal design becoming more and more important.

12.2 Information about master thesis and anonymity

Master thesis: Describe the objective with the master thesis, what we would like to get out of it, how we have planned to carry it out and how long time the user test is going to take. Ask if participant want us to read the information letter that was sent to them. **Anonymity:** Tell the participant that all information collected in the interview and user test will be kept strictly anonymous both in the final report and presentations. The user can at any point say that he/she will not be part of the experiment. The user can at any point in time after the test is finished ask for all the data to be deleted.

Ask if the participant have any further questions before we start.

12.3 General information and background information about the participant.

Participant number: Date: Age: Gender: Constriction/disability:

12.4 Information about experiment and prototype

Tell the participant about the two key solutions and how you can enter pin codes with it. The key pad is using the two buttons next to the zero key found on most numeric keypads. These keys sometimes is used for moving up and down in menus and sometime to enter star () or hash (#) but most of the time they are not used at all. These keys are used because we believe it would make it possible to reprogram the payment terminals without doing anything with the device itself. Number of presses on the first button tells the number (e.g. the number 4 is entered with pressing the first key 4 times). To indicate that a number is entered press the second key to move to next number. The number zero (0) is entered by just pressing the next key (e.g. the pin code 0000 is entered with 4 presses on the next key. When the pin code is entered the OK/Return key is pressed to start the validation process. Before we start the real test you will be able to try the method if you like. The experiment will try to measure if this new pin entry method is easy to learn, understand and use by everyone. The two button method will hopefully have some benefits like easy to locate by people with visual disabilities, usable with only one hand and have a security improvement for everyone because it will not be possible to shoulder surf and by that see what pin that is entered. In the experiment we will first monitor a normal pin entry method where the user enter the pin code by typing the pin with the numeric keys, in the second part we will use the new pin entry method. In the test you will enter two different pin codes, one selected by you and one selected by us. Please do not select your normal pin code even when we have no interest in collecting it. We will use a video camera and film your hand during the experiment. This video will be analysed afterwards to see if it is still possible to figure out what the entered pin(s) are.

12.5 General questions before test start

What is your experience with the usability of ATMs? What is your experience with the PIN entry when using ATMs? What is your experience with the usability of payment terminals? What is your experience with the PIN entry when using ATMs? When using ATMs and Payment terminals what security incidents do you think could happened? When using ATMs and payment terminals what security precautions do you take if any?

Questions only for people with disabilities: What is your experience with accessibilities and ATMs? What is your experience with accessibilities and payment terminals?

12.6 Test of prototype

Set up test Enter information about the test person and let them select a PIN code by them self. Start test Enter self-selected pin tree times with the numeric keys. Enter our pin code tree times with the numeric keys. Enter self-selected pin tree times with new input method. Enter our pin code tree times with new input method. Save test and exit

12.7 General questions after test

What is your general experience with this PIN entry method? What was the main drawback with it when it comes to usability and accessibility? Have your heard of other methods for authentication in ATMs and payment terminals?

12.8 Closing information

Tell participants that I will send them my minutes from the questions afterwards so they can give comments if they have any. Offer them to send them my final report when it is finished.