User's trust in Biometric Authentication Systems

– Do not take the end-users for granted

Henning Gravnås

Master's Thesis
Master of Science in Information Security
30 ECTS
Department of Computer Science and Media Technology
Gjøvik University College, 2005

The MSc programme in Information Security
is run in cooperation with the Royal Institute
of Technology (KTH) in Stockholm.

Institutt 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

The last years there has been a stronger focus on security in the media all over the world. One of the important issues in security is the need of correctly authenticate a person. This is possible either by providing something you know (e.g. password), something you have (e.g. ID-card), or something you are (e.g. biometrics). This study explores to what extent possible users of a biometric authentication system have trust in such a system. The participants in this study have answered several questions regarding the issue, as well as witnessed how a biometric authentication system works and how it can be fooled. By using a simple method of making artificial fingerprints, the system was fooled. The method is described in this report. The results from the questionnaires have been analyzed and discussed against three hypotheses which allege that a user quickly will accept and have trust in a biometric authentication system. The hypotheses also allege that the user will change his or her trust when witnessing how easily such a system can be fooled. The study shows the users trust for the most common biometric techniques, and how the trust changes when the weaknesses of one of them are demonstrated.

Keywords: Information security, biometrics, fingerprint recognition, authentication, verification, attitude, trust, privacy, user experience.

Sammendrag (Abstract in Norwegian)

I de senere årene har mediefokuset vært rettet mot sikkerhet. Et av kravene innenfor sikkerhet, er økt behov for korrekt autentisering av en person. Det er mulig å autentisere seg ved å fremlegge bevis på noe du vet (for eksempel et passord), noe du har (for eksempel et ID-kort) eller noe du er (for eksempel biometri). Denne undersøkelsen forsøker å finne ut av i hvilken grad mulige brukere av biometriske autentiseringssystemer har tillit til et slikt system. Deltakerne i denne undersøkelsen har besvart ulike spørsmål om dette temaet, og har i tillegg sett hvordan et biometrisk autentiseringssystem virker og hvordan det kan lures. For å lure systemet ble deltakernes fingeravtrykk kopiert ved bruk av en enkel metode beskrevet i rapporten. Resultatene fra undersøkelsen har så blitt analysert og diskutert mot tre hypoteser som påstår at en bruker av et biometrisk autentiseringssystem lett vil få tillit til det, men at tilliten svekkes når man ser hvor lett systemet kan lures. Undersøkelsen viser brukernes tillit til de mest vanlige biometriske teknikkene, og hvordan tilliten endres når svakhetene ved en av dem demonstreres.

Nøkkelord: Informasjonssikkerhet, biometri, fingeravtrykk gjenkjenning, autentisering, verifisering, holdning, tillit, personvern, brukeropplevelse.

Acknowledgements

I would like to thank my contacts at the hospital, Kai Kristiansen, Børge Sandstedt, and Anne Grethe Mathisen who have been very helpful in finding, organizing and briefing the participants, and collecting questionnaires. I would also like to thank the participants at the hospital, whose names cannot be mentioned here due to privacy concerns. I would also like to thank my teaching supervisor at GUC, Kirsi Helkala. Your evaluations on the different parts of my work, helping tips on statistics and different approaches to the material have been very valuable, not to mention your interest in the topic and the result of this study. Thank you.

Finally I would like to thank my friends and family for backing me up, and having patience when I have had to reschedule different activities due to working on this thesis. Thank you all!

Preface

Research on biometric authentication is one of the many interesting issues in the world of information technology. Gjøvik University College (GUC) offers a 1/2 semester course on authentication and one of the issues introduced is biometric authentication. I found the topic very interesting, and wanted to explore it further.

Fingerprint authentication is a rapidly growing technology, and is more and more used instead of or together with traditional authentication. Sykehuset Innlandet has considered this technology, and for them it will be valuable to know what the employees think about this form of authentication versus the traditional passwords and ID-cards.

The work in this study has been carried out with help from participants at Sykehuset Innlandet, Gjøvik.

This thesis is the final work at GUC, and covers one semester. The study and production has to be one's own, but it is possible to use resources at GUC and NISlab especially. Except from exact citations from sources, which have been referred to, all the work in this thesis is my own, or based on inspiration from ideas of my thesis adviser.

This last year has been full of new situations for me, and it has been interesting working on such a big paper. I feel I have learned and developed a lot, both academically and socially.

Gjøvik 01.07.2005

Henning Gravnås

Table of Contents

List of Figures

List of Tables

1 Introduction

This chapter contains a short introduction of the topic of the thesis as well as a description of what problem the thesis wants to answer. The goal, purpose and target group, who will benefit from the project, will be presented here. Any limitations of the project will be covered in the last part of this chapter.

1.1 Topic covered by the thesis

Security is becoming more and more important in today's world, and because of this, the need of authentication in day-to-day situations has become more important than earlier. A growing field of authentication and security is the use of biometric systems for personal authentication [Mans], and fingerprint recognition is the mostly used method [Sand]. A fingerprint is generally known to be unique for each individual, even for identical twins [Jain], and is therefore thought of as a secure solution for authentication. However, studies have shown that a fingerprint sensor device can easily be fooled by the use of an artificial finger, which holds a copy of the original fingerprint, [Blom], [Mats] and [Putt]. Are potential users of biometric recognition systems not aware of this weak point, and therefore have more trust in such systems? This thesis will give an indication to how this situation is today.

1.2 Problem description

Because of the rapid evolution in technology, demands to protection of privacy, and not at least actions of terrorism, issues regarding security have been shown more attention the last years. One of the major problems with increased security is that the user experience is often decreased and vice versa. When a user logs onto a system, one or several passwords are required, and the password(s) might be hard to remember. This decreases user experience because a user needs to remember different passwords, PIN-codes and user names. Maybe they also need to be changed often, to increase security, which means that they are easier to forget. This issue might decrease security, because users tend to choose easy-to-remember passwords, or they simply write it down on a note, and "hide it" under the keyboard or similar.

In an attempt to increase security and user experience, research on biometrics to do a correct identification or verification has shown great development the last years. Its goal is to develop systems which are reliable enough to correctly authenticate a user based on his or her biometric data. The system should also not give access to non-authorized users.

A research performed by the European Commission in 2003 [Euro], looks at what view citizens of the European Union (EU) have about privacy and information security. It also explores what level of trust the citizens have of different businesses managing their private information. The research shoes that especially the Nordic countries have a high rate of trust on different questions concerning privacy. One of the interesting issues is then to find out to what extent potential users of biometric authentication systems are willing to register their data, and let the system make use of these data. Is it possible

that the users are willing to sacrifice some lack of privacy if it makes it easier and more secure for them to gain access to a system? Another question that arises is whether the users are aware how sensitive their different biometric data actually are, and if they are uncritical or maybe ignorant to the use of this kind of information.

1.3 Project goal, purpose and target group

An earlier study [Helk], carried out at Sykehuset Innlandet by Gjøvik University College (GUC) explores issues when it comes to user authentication. The situation at the hospital today is that many of the users are required to remember several usernames and/or passwords and these have to be changed from time to time. There is no guarantee that these passwords are required to be changed at the same time, which complicates the situation for the users even more. A single-sign-on system would have simplified the situation when it comes to user convenience, but this is not a secure solution since the users might know each others passwords. The hospital has considered biometric authentication as a supplement or replacement for the traditional authentication systems, and the goal with this project is to do a research on possible end-users' trust, attitudes, and possible demands to biometric authentication versus traditional authentication.

It is important that a biometric authentication system not only is secure and easy-to-use, but its users also need to have confidence and trust in the system. The research in this thesis will examine to what extent potential and/or existing users of a biometric authentication system trust that their information is stored and used in a properly and secure way. Are they under any circumstances positive to use such a system? By examining this, it might be possible to see an indication on whether more information is needed for the average user before such a system is implemented.

There are different target groups who can find this thesis beneficial:

- Sykehuset Innlandet, which considers implementing biometric authentication systems, and others who plans to implement a biometric authentication system from the start or as a supplement or replacement to traditional authentication
- Developers of biometric authentication systems who are concerned about user interaction
- Current and possible new users of biometric authentication systems
- Everyone who has an interest in computer science, especially security and biometrics
- Researchers and other thesis-students who plan to do a study in biometric authentication systems, and user interaction

1.4 Hypotheses and research questions

The thesis examines the following hypotheses:

- H1: End-users will quickly accept biometric authentication systems.
- H2: After a demonstration on how a biometric authentication system can be fooled, end-users will change their opinion of such an authentication system to a lower level of trust.
- H3: End-users are not aware of, or have knowledge about privacy and technology issues to set requirements to registration, storage, and management of their biometric information.
-

To investigate these hypotheses, answers to the following research questions have been answered:

1. What types of biometric information can be registered and used to authenticate a user?
2. What are the advantages and disadvantages of the different biometric characteristics?
3. What does a biometric authentication system demand from the users?
4. How comfortable are the users about capturing, registering, storing, and using of their biometric information?
5. How acceptable do the users think it is to demand registration of biometric information for authentication in a system?
6. What do the users think about biometric- versus traditional authentication?
7. What techniques do the users feel is a secure form for authentication?

1.5 Method

The method used in this study is in literature referred to as a mixed method approach. A mixed method approach is a combination qualitative- and quantitative research methods, and makes use of these two methods when collecting and analyzing data [Cres]. The qualitative method has been used in the literature study while the quantitative method has been used in the survey to analyze the results.

1.5.1 The survey

By this study the author wishes to explore possible end users points of view when it comes to biometric authentication systems. The study will focus on security, usability, privacy, and acceptability issues. A group of employees at 'Sykehuset Innlandet, Gjøvik' were asked to participate in the study. All participants were required to read an

information letter and sign a letter of agreement which stated the "rules" of the study, see Appendix B. The participants had the chance to cancel parts of the study they did not want to participate in, for example the molding of their fingerprint.

The description of the study is in Chapter 4.

1.5.2 The questionnaire

Chapter 1.4 presented the hypotheses and research questions for this experiment. The reason for doing the survey is to investigate these research questions and examine the hypotheses. The complete questionnaire is provided in both Norwegian and English in Appendix A.

Because of the different questions asked, it is possible to separate the participants into several different groups, and it might also be possible to determine if one factor is dependent on another. The questionnaire first asks for demographic data. These questions cover such factors as age, sex, department, if the participant has studied IT, how often the participants uses computers in his or her daily work, if and how they authenticate for systems at work, and if they ever have told their password to someone or have lent out their personal ID-card. These variables can be said to be stable variables because they should not change between the two sessions. It is, however, important to register this information so differences or similarities between groups, e.g. people of the same sex, can be discovered. For example there can be signs that there exists a difference between male and female participants on some of the questions in group two. The goal is to find out if this difference is significant.

The second group of questions consists of questions that are alterable, or susceptible to influence. These questions explore personal thoughts from the participants, and attempt to reveal what the participants think and feel about biometric authentication. Issues like how comfortable they are with registration and use of their biometric information, how acceptable it is to demand registration of biometric information, how they would rate biometric authentication versus traditional authentication when it comes to ease of use and security, and what authentication techniques they feel is a secure form of authentication. It is important to see if the answers to these questions change during the period of the project, and if they do, find out if the change is significant.

The results from the survey are presented in Chapter 5, and analyzed, and discussed in Chapter 6.

1.6 Limitations

The duration of the project has been limited to one semester, approximately six months. In a study like this, several issues might be interesting to explore. Many of these

however, were found either to take too long time, or they emerged too late in the study to be implemented. Many of these are instead discussed in Chapter 8 and proposed as recommendations for further work.

This project has not been sponsored in any way, so the author has covered all expenses himself. It has therefore been intentional to keep any expenses as low as possible. See also Chapter 4.4 for factors that were important when choosing material for the study.

The fingerprint sensor used in the experiment is an optical sensor since this is one of the sensors available at the information security laboratory, NISlab, at GUC.

All the participants were recruited at the Hospital of Gjøvik, 'Sykehuset Innlandet, Gjøvik' since GUC already has performed earlier studies at the hospital, and the hospital has been considering implementing biometric authentication. Due to privacy rights, none of the participant will be mentioned by name, and it shall also be impossible for one single participant to be recognized from his or her answers in the study. For more on this, see Chapter 4.4.5.

1.7 Reading guide

The reading guide will make it easier for the different target groups to navigate through the report and find the most relevant part of their interest.

Part 1 (Chapter 1) introduces the thesis work, and presents the background of the thesis as well as providing general information.

Part 2 (Chapters 2 and 3) provides background information in the field of authentication and biometrics, earlier work, and the situation of today. Most of the topics here are background information describing terms used in the thesis so any reader will have a better understanding of the rest of the thesis. Some of the terms described here are, however, not discussed later in the thesis, but the author found it necessary to provide this information because it is essential for the understanding of the field of biometric authentication.

Part 3 (Chapter 4) describes the survey and demonstration in detail, so that everyone who wishes can carry out a similar study at a later stage.

Part 4 (Chapters 5 to 8) presents the results from the questionnaires, an analysis and discussion of the results, draws a final conclusion and proposes possible improvements for further research.

- Chapter 1 introduces the reader to the topic, the problem of the situation of today,

the purpose, goal and target group of this research. The hypotheses and the research questions are presented, together with the method used for this study, and any limitations. The chapter also provides this reading guide so the reader easily can find the part that suits their interest.

- Chapter 2 gives the reader an introduction to the authentication term and describes other relevant important terms under this subject.
- Chapter 3 describes the different biometric characteristic, e.g. fingerprint, hand geometry, eye, voice and signature.
- Chapter 4 gives a closer description on how the survey was carried out, who the participants were, and how the system was set up. The way the artificial fingerprint was made is also covered here. The chapter also mentions any privacy issues of the study.
- Chapter 5 presents the results from the survey.
- Chapter 6 analyzes and discusses the results and possible errors from the demonstration and the survey.
- Chapter 7 contains a final conclusion based on the results from the survey.
- Chapter 8 suggests possible improvements to the survey and experiment, and presents ideas for further research in the subject of this thesis.
- The bibliography contains the different sources that have been used as support for the work in this thesis. Additional material used in or produced by the study is attached in the appendixes.

1.8 Notes

Different terms have been used in this paper:

- 'The' or 'this report' and 'the' or 'this paper' refer to this paper.
- 'The study' refers to the thesis work that has been done by the author of this paper over the last year, ending up in this report.
- 'The survey' refers to the interaction with the participants at the hospital, where they used a fingerprint authentication system and saw a demonstration of how it is possible to fool such a system.
- 'The questionnaire' refers to the set of questions the participants were required to answer.

2 Authentication background

Every one of us has distinct features which make a person unique. As we go about our daily lives, we make use of these features to help us identify or verify other peoples' identities or verify our own identity. An identity in the world of computer technology is defined as "the unique name of a person, device, or the combination of both that is recognized by a system. Many types of systems rely on unique identities to ensure the security of networks and resources" [Web10]. A common synonym for identification and verification is authentication.

The situation in the world today has made security become more and more important, and because of this the need to authenticate in day-to-day situations has become more important than earlier. Tragic events like the terrorist attack on the twin towers in New York on September 11, 2001 has made people more aware of their own safety and privacy, especially in their physical life, but also in the world of computers and technology. This means that "a wide variety of systems require reliable personal recognition schemes to either confirm or determine the identity of an individual requesting their services" [Jain2].

When a system or a person validates the identity of another person or a system, an authentication process is performed. This means that anyone who is authenticated should be able to declare that they are who they claim to be. It is however important to know that an authentication process only verifies the identity, it has nothing to do with what the identity is authorized for. Or as [Web6] states; Authentication is "The process of identifying an individual, usually based on a username and password. Authentication ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual". In their working draft titled "1st Working Draft – INCITS M1 Vocabulary Harmonization", the InterNational Committee for Information Technology Standards (INCITS) defines authentication as " The process of determining an individual's identity, either by verification or by identification. A security measure that verifies a claimed identity. The preferred biometric term for authentication is 'verification' " [INCI].

The next section will describe these two different types of authentication.

2.1 Identification and verification

Authentication of an individual can be performed in two different ways, identification and verification [Phil] and [INCI].

2.1.1 Identification

In an identification system the user does not have to claim an identity. The authentication system searches the entire database for a match. This is called a 1: N (one-to-many) process of authentication, because a person's identity is determined by performing matches against multiple biometric templates [Web9] and [Boll]. In a biometric security system identification is defined as "the process of comparing a biometric data sample against all of the system's databased reference templates in order to establish the identity of the person trying to gain access to the system", [Web3]. A typical example might be a surveillance camera searching for known terrorists at an airport. The camera scans an area for people's faces, and sends any captured images to the authentication system, which compares the images to a database with images of known terrorists.

2.1.2 Verification

In a verification system a user claims an identity, and usually provides a proof for the system to confirm the identity. This is called a 1:1 (one-to-one) process of authentication, because the validity of a claimed identity is established by comparing a verification template (the claimed identity of the user) to an enrollment template (the identities known to the database of the authentication system) [Web9] and [Boll]. In a biometric security system verification is defined as "the process of comparing a biometric sample against a single reference template of a specific user in order to confirm the identity of the person trying to gain access to a system", [Web4]. Another typical, and very common, example is when a user logs on to a computer at work. He or she will then be asked for a username and password, the system will then find the matching username in the database and verify if the entered password matches the one stored with the username in the database. A verification system needs interaction with the user.

Both these two types of authentication are used in biometric authentication systems, and are chosen depending on the application context [Malt].

With both ways, the system needs a stored template of the individual's specific information. This is because the system needs something to compare the entered information with, and this information can either be something the individual knows, has, or is (see Chapter 2.2). The system will then either reject or accept the attempt to authenticate depending on whether the entered information matches the stored template or not. Figure 1 shows how a biometric verification system works.

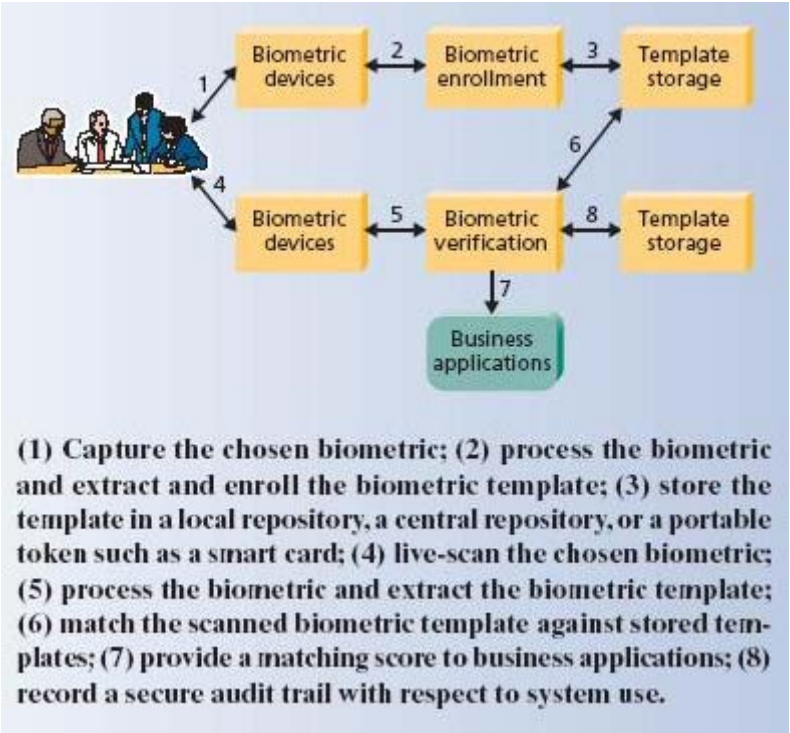


Figure 1: How a biometric verification system works [LiuS].

A biometric authentication system will also operate in either of two modes:

Positive recognition

"The system establishes whether the person is who he (implicitly or explicitly) claims to be. The purpose of a positive recognition is to prevent multiple people from using the same identity" [Malt]. For example, if only the director of the hospital is authorized to view certain files or journals, the system will grant access only to the director, by accepting the input given. If someone else attempts to view the files, they will be rejected by the system.

Negative recognition

"The system establishes whether the person is who he (implicitly or explicitly) denies being. The purpose of negative recognition is to prevent a single person from using multiple identities" [Malt]. [Web7] defines negative identification as "evidence proving that you are not who you say you are; evidence establishing that you are not among a group of people already known to the system; recognition by the system leads to rejection". For example, if Charlie's application for a US green-card is denied, he should

not be able to claim that he is Bob and receive a green-card in Bob's name. In this situation the system will establish that Charlie is not who he claims to be (he is not Bob). It is important to know that "negative identification can only be accomplished through biometric identification. If a PIN or password is lost or forgotten it can be changed and reissued but a biometric identification cannot" [Web1].

Thus, positive recognition modes can operate both in a verification system and an identification system, since it will return a result when it finds a match, but negative recognition mode can only operate in identification mode, since it has to search the whole database of templates to prove that the given input is not among the already known templates.

2.2 Methods of authentication

In the field of authentication today, there are currently three methods to authenticate oneself to another person or a system.

2.2.1 Knowledge-Based ('what you know')

Knowledge-Based authentication relies on the user to remember something. This can e.g. be a password, a PIN-code or an address. Security is a huge drawback because it is very easy either to guess a password (lots of users chose passwords that are easy to remember, such as birth-dates, names of children etc) or find a password that is written down. "All it takes is for someone to overlook or overhear you mentioning this secret information. Since nothing else than a memory is required, it is now easy to use this to your advantage" [Blom]. It can also include information that is not so much secret as it is 'obscure', which can be loosely defined as 'secret from most people'. "A security drawback of secrets is that, each time it is shared for authentication, it becomes less secret" [Gorm]. Another drawback is user convenience, because to maintain a certain level of security, users have to change passwords now and then. They often have to choose passwords that are difficult to remember, and/or they cannot choose a password that is similar to a password entered earlier. Studies have been done on how to make such systems easier for the users, while still keep up with security [Bros].

2.2.2 Object-Based ('what you have')

Object-Based authentication relies on the user to be in possession of something, e.g. a token. This can typically be a VISA-card, a passport or an ID-card. This method is often compared to using a metal key to access your house. Object-Based authentication is therefore an easy solution that is practical in its use, because the users normally don't need to remember a password. The drawback with this method is, as with the Knowledge-Based method, security. These items or tokens can easily be stolen and later on used or copied, sometimes with the user unaware of the copying process. By copying

for example an ID-card, an intruder gains access to formerly restricted areas or information.

"A security drawback of a metal house key is that, if lost, it enables its finder to enter the house. This is why many digital tokens combine another factor, an associated password to protect a lost or stolen token. There is a distinct advantage of a physical object used as an authenticator; if lost, the owner sees evidence of this and can act accordingly" [Gorm]. As Gorman argues, a combination of the Knowledge-Based and the Object-Based methods provides greater security than by using only one of the methods alone.

Research on Smart-Cards is growing, and developments and studies show that this form of object-based authentication is very safe [Abbo] [Basi].

2.2.3 ID-Based/Biometric-Based ('who you are')

ID-Based authentication relies on the user to have specific biometric characteristics. This can typically be fingerprints, iris or retina, DNA or even voice (see Chapter 3). Biometric-Based authentication relies on something that belongs to you (your body), and therefore these data can not easily be stolen. "Since you can not change these details, a successful forgery might prove to be unstoppable since you cannot change your biometric information" [Blom].

Biometric authentication is defined as "the automatic identification of living individuals by using their physiological and/or behavioral characteristics" [Web1] and [Jain2]. The Biometric Group and the International Biometric Industry Association provides the same definition, but also includes verification in addition to identification [Web8] [Web20].

Biometric authentication is in many ways more convenient than the other two methods. Your fingerprint is something that always is with you, and you don't have to remember or change it. This is why biometrics is believed to replace or at least supplement the other two methods within short time. However, there are some drawbacks, as Gorman describes: "For both ID-documents and biometrics, the dominant security defense is that they are difficult to copy or forge. However, if a biometric is compromised or a document lost, they are not as easily replaceable as passwords or tokens". Imaging fingerprint authentication being used when entering your house, paying for groceries at the local store, or entering a passport control. It sounds very convenient, but imagine that someone has followed you for a couple of days, picking up whatever you touch with your fingers. It might be a glass of beer at the local pub, the button you pressed in the elevator or the carrier you put your groceries into. All of them might have a decent copy

of your fingerprint. You don't know if anyone has a copy, and you can't change your finger either. The person that followed you has now stolen your identity, and might, depending on the security of the authentication system, pretend to be you. It is a security drawback indeed. For more information on biometrics characteristic, see Chapter 3.

The following table summarizes the three different methods of authentication:

Authentication method	Knowledge based	Object based	Id-based
Commonly known as	Password, secret	Token	Biometrics
Example of use	User logon with password on a computer	Access to a building by using an Id-card	User logon with fingerprint on a computer
Examples of user requirements to support security	Secrecy, do not tell it to anyone, do not choose easily guessed passwords	Possession, keep the token to yourself, and store it on a secure place	Uniqueness, be sceptical on where you register your biometric data
Security issues	Less secret with each use, someone can eavesdrop or guess the password, often difficult to know when it is lost	Can be misused if lost, gains easy access, often easy to know when it is lost	Difficult to replace your biometric data if they are copied, often difficult to know when it is lost
Examples of other method(s) the method can be combined with	Often combined with the object based method, i.e. a PIN-code and an ID-card	Often combined with knowledge based or ID-based	Often combined with the object based method, i.e. a fingerprint and a passport

Table 1: Summary of the three methods of authentication, inspired by [Gorm].

2.3 Other terms used in an authentication process

The process of acquiring a biometric sample from a user is in a biometric authentication system called capturing [Web11]. The captured biometric information is then extracted, which means that it is converted into data that can be compared to a reference template [Web14] that represents the biometric measurement of a specific person's identity [Web13]. By capturing and collecting biometric data samples from a person and subsequently storing the data in a reference template representing a user's identity to be used for later comparison will enroll this person in the system [Web12]. This reference

template is then stored on to a local repository, a central repository, or to a portable device such as a smart card or passport [LiuS] and can be used for authentication at a later stage.

The process of authenticating (verifying) a user in an authentication system will require some sort of biometric information input from the user. This can be done with a biometric capturing device, such as a fingerprint device or a camera. The input is captured, extracted, and compared with the stored reference template. This is called matching [Web15]. After the matching process, the system assigns a score based on the level of similarity between the two templates. The biometric system then issues an accept- or reject-decision based on the results of the matching [Web15].

When anyone wants to estimate how good a biometric recognition system is, the False Acceptance Rate (FAR), False Rejection Rate (FRR) and Equal Error Rate (EER) are measured. These rates can be found by testing the equipment and application(s) as it would be in normal use. To find the rates for a specific system, for example a fingerprint recognition system, every attempt to authenticate to the system, and the outcome of the attempt, must be recorded.

The following terms are used in the field of biometrics to describe a biometric recognition system's recognition rates.

2.3.1 False Acceptance (Rate)

A false acceptance occurs when the authentication system incorrectly verifies or identifies an unauthorized user [Web16]. If a fingerprint recognition system matches a provided fingerprint of a user that isn't authorized with one of a user that is authorized, the unauthorized user gains access to the system, and a false acceptance has occurred. "The false acceptance rate (FAR) is the ratio of the number of instances of pairs of different fingerprints found to (erroneously) match to the total number of match attempts" [Boll]. "FAR is the measure of the likelihood that the system will incorrectly accept an access attempt by an unauthorized user. FAR is typically stated as the ratio of the number of false acceptances divided by the number of identification attempts" [Web16]. False acceptance is also referred to, what in statistic is denoted as a Type II error, because it gives unauthorized users access to systems that are trying to "keep them out". This is therefore considered the most serious of biometric security errors. False acceptance is also often denoted as "false match" because the system is mistaking biometric measurements from two different fingers to be from the same finger [Malt].

2.3.2 False Rejection (Rate)

A false rejection occurs when the authentication system fails to verify or identify an authorized user [Web17]. If a users biometric information is correctly enrolled into a systems database of templates, but the user isn't recognized when providing a fingerprint on the scanner, a false rejection has occurred. There are several reasons why a false rejection might occur, the enrolled template(s) can be of bad quality or the provided template, used to authenticate, can be of bad quality, or the conditions and surroundings, such as the weather or light can be different. "The false rejection rate (FRR) is the ratio of the number of instances of pairs of the same fingerprint are found not to match to the total of match attempts" [Boll]. "FRR is the measure of the likelihood that the system will incorrectly reject an access attempt by an authorized user. FRR is typically stated as the ratio of the number of false rejections divided by the number of identification attempts" [Web17]. False rejection is also referred to, what in statistics is denoted as a Type I error, because it denies authorized users access to systems they are allowed to use. This is not as serious an error as the false acceptance error, but is fully an error. It keeps authorized users out, and can cause frustration and bad user experience especially in cases where the user needs the information fast. False rejection is also denoted as a false non-match because the system is mistaking two biometric measurements from the same finger to be from two different fingers [Malt].

It is important to notice that while the terms false match and false non-match are not application dependant, false acceptance and false rejection are. In a positive recognition system, an impostor (someone who uses a false finger for example) is determined by the false match, while a false non-match causes the false rejection of an accepted user. In a negative recognition system, however, a genuine request is rejected by a false match and an impostor attempt is falsely accepted by a false non-match. "When using a biometric system, one would of course want to minimize both rates, but unfortunately these are not independent. An optimum trade-off between FRR and FAR has to be found with respect to the application" [Putt]. This is commonly known as the equal error rate.

2.3.3 Equal Error Rate

"A biometric security system predetermines the threshold values for its FAR and its FRR, and when the rates are equal, the common value is referred to as the equal error rate." [Web18]. As Figure 2 shows, EER is the value where the FAR and the FRR values are equal. Where false rejection is high, "High Security Access Applications" typically operate while where false acceptance is high "Forensic Applications" typically operate. At EER most of the "Civilian Applications" operate. [INCI] defines EER as "The probability or percentage of errors when the decision threshold of a system is set such that the false match rate is equal to the false non-match". An earlier synonym for EER is crossover error rate.

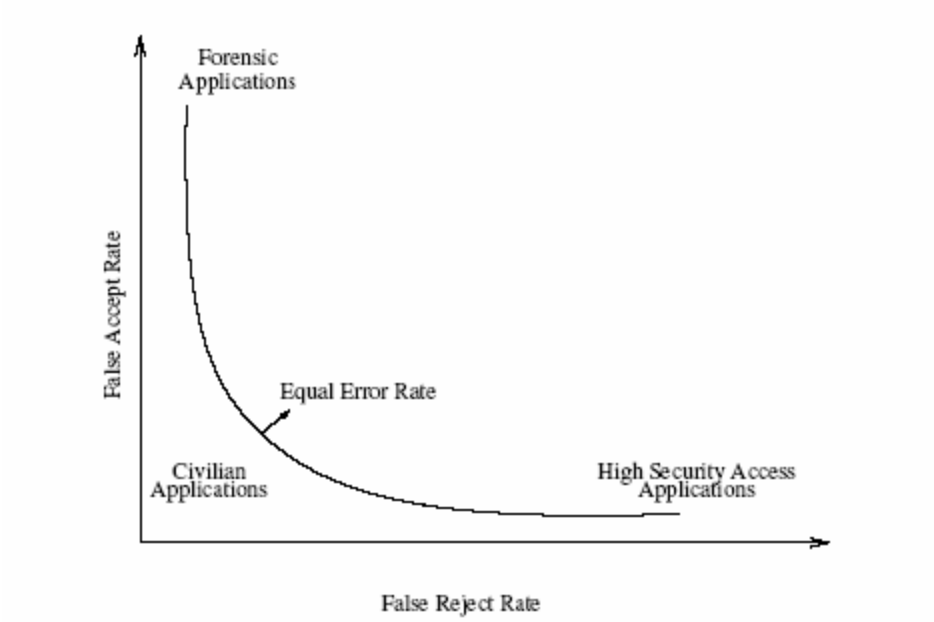


Figure 2: The relationship between FAR, FRR, and EER, illustrated on a Receiver Operating Characteristics (ROC) curve. Source: [Boll].

3 Biometric background

It is impossible to design a "perfect" authentication system. Depending on the situation for which the system will be used, what biometric characteristic is suitable to use, how secure the system should be etc. an implementation of a biometric authentication system will have a wide array of different factors to choose from. This chapter provides some background and theories on what identifiers that should be considered when it comes to implementing a biometric authentication system, and what biometric characteristics are available for such a system.

3.1 Biometric identifiers

For an authentication system to be as good as possible there are several requirements that must or should be satisfied. Jain et. al. and Maltoni suggest that a "perfect" authentication system ought to satisfy the requirements of universality, distinctiveness, permanence and collectability. For a biometric authentication system to be practical, they also suggest that performance, acceptability and circumvention also should be considered. Garcia et. al. add some more factors including reliability, ease of use, ease of implementation, and cost. The different requirements mentioned will be further explored in Table 2.

Requirement	Description	Problem(s)	Source(s)
Universality	Universality means that every person should have the biometric identifier.	People who has lost a body part that is needed as a biometric identifier.	Maltoni et. al., and Jain et. al.
Distinctiveness	Distinctiveness means that any two people should be sufficient different in terms of their biometric identifiers.	Identical twins have identical DNA structure.	Maltoni et. al., and Jain et. al.
Permanence	Permanence means that the biometric identifier should be sufficiently invariant (with respect to the matching criterion)	Wounds can alter a finger or a face, voice and face changes over time	Maltoni et. al., and Jain et. al.

	over a period of time.		
Collectability	Collectability indicates that the biometric can be measured quantitatively.	How determine which biometric data are easiest to collect?	Maltoni et. al., and Jain et. al.
Performance	Performance refers to the achievable recognition accuracy, speed, robustness, the resource requirements to achieve the desired recognition accuracy and speed, as well as operational or environmental factors that affect the recognition accuracy and speed.	There are several biometric authentication systems for the different biometric characteristics. Which one is the better one?	Maltoni et. al., and Jain et. al.
Acceptability	Acceptability indicates the extent to which people are willing to accept a particular identifier in their daily lives.	Lots of people do not want to register their biometric information because they consider it to be too personal.	Maltoni et. al., and Jain et. al.
Circumvention	Circumvention reflects on how easy it is to fool the system by fraudulent methods.	Some biometrics are easier to copy than others, for example fingerprints or mimicking a voice.	Maltoni et. al., and Jain et. al.
Reliability	Reliability refers to sensor noise, limitations of the processing methods, and the variability in both the biometric feature as well as the presentation may trigger a non-match in the authentication process. "The accuracy of a given biometric implementation is sensitive to the target population", and "to apply a biometric technology	No system is 100% secure or reliable, and there will always be room for improvement.	Garcia et. al.

	successfully, it is important to understand and evaluate the technology in context of the target application and the target population" [Waym].		
Ease of use/practicality	Ease of use refers to how easy the biometric authentication system is in use for the users. "In order for a biometric identification system to be practical the difficulty of using and learning how to use (training) the system must explicitly be addressed in the context of the target application and potential users" [Garc].	Can the system be too simple, so the users do not think about the security aspects?	Garcia et. al.
Ease of implementation	Ease of implementation indicates that the biometric technology must be made easily accessible for system integration and implementation.	It might be difficult to integrate a new system into already existing systems, and the implementation might also be expensive.	Garcia et. al.
Cost	Cost indicates that there are a number of issues to consider when estimating the total cost to deploy a biometric system. Equipment, installation, and training, software and system maintenance and	Several issues to consider when a cost analysis is performed. Difficult to measure cost of lost reputation etc if a biometric authentication system fails.	Garcia et. al.

	operation costs should be considered.		

Table 2: Requirements a biometric authentication system ought to satisfy.

3.2 Biometric characteristics

Our body consists of several characteristics that can be used for biometric authentication, and the characteristics may have different strengths and weaknesses (see Chapters 3.3 and 3.4). Easily explained, biometrics is the automated use of physiological or behavioral characteristics to determine or verify someone's identity. Thus biometric characteristics can be divided into two groups, physiological biometrics and behavioral biometrics [Putt]. It is important to know that "behavioral biometrics are based in part on physiology, such as the shape of the vocal chords (voice recognition) or the dexterity of hands and fingers (signature-scan)" while "physiological biometric technologies are similarly informed by user behavior, such as the manner in which a user presents a finger or looks at a camera" [Web8].

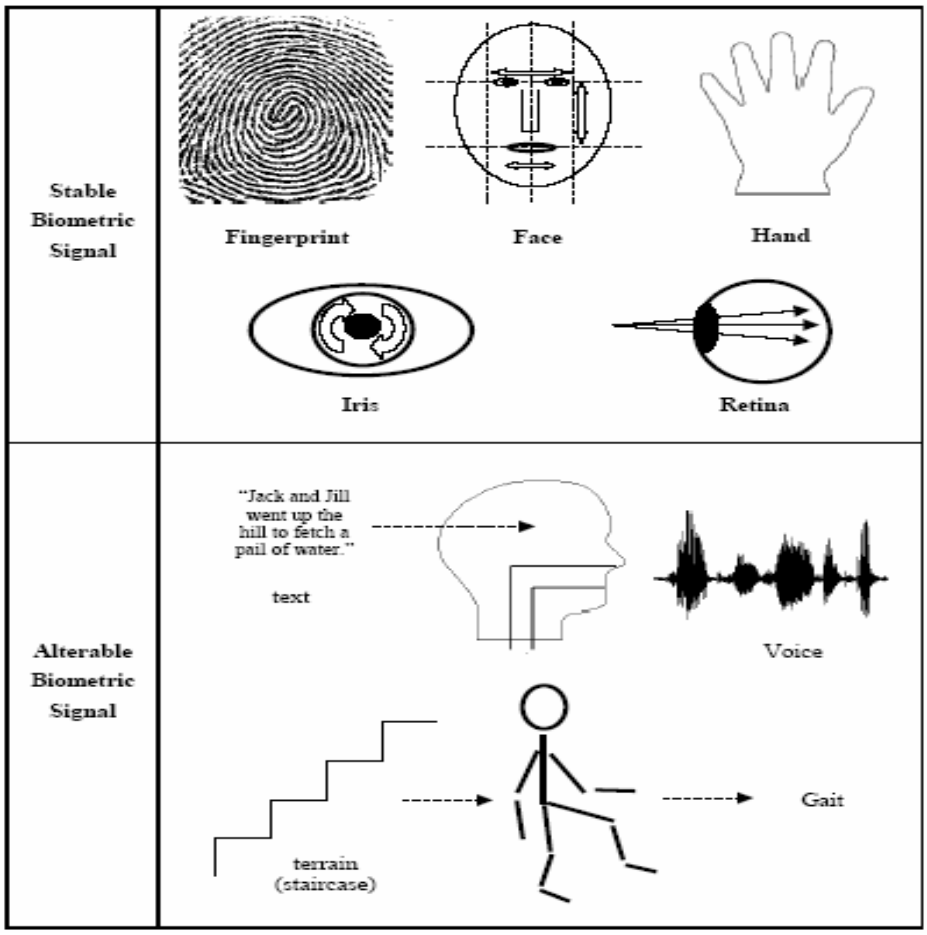


Figure 3: Examples of stable and alterable biometrics, source [Gorm].

Gorman therefore suggests a different classification which doesn't involve the physical and behavioral labels. The idea is not to classify the biometric characteristic, but rather the biometric signal. According to Gorman there are two different biometric signals, "Stable biometric signal" and "Alterable biometric signal" [Gorm], as shown in Figure 3. These two signals will be described in the next sections and the most regular biometric characteristics will be classified into either.

3.3 Physiological biometrics

[Web8] provides the following definition on physiological biometrics: "Physiological biometrics is based on measurements and data derived from direct measurement of a part of the human body". Physiological biometric characteristics are in literature also

denoted as a stable biometric signal. This is because the captured "biometric signal" is relatively constant in time [Gorm]. The biometric signal can often be captured in an image, such as a fingerprint or an image of someone's face. Examples of physiological biometrics are fingerprint, iris-scan, retina-scan, hand geometry, and facial recognition.

3.3.1 Fingerprint

When you touch something with your fingers, you leave a specific impression on the touched item. This is called a fingerprint, or as [Web23] defines: A fingerprint is "an impression on a surface of the curves formed by the ridges on a fingertip, especially such an impression made in ink and used as a means of identification".

A foetus's fingerprints are normally fully developed already after seven months. Except for big injuries, disease or decomposition after death the specific characteristics on one's fingerprint does not change throughout a lifetime [Sand]. The patterns on a fingerprint will also grow back to normal as the finger heals from a small injury [Malt].

History

The studies of fingerprints go long back, and it is not possible to decide who first discovered the features that a fingerprint can provide. A summary of the most important history of the research on fingerprints as an identification tool is provided in Appendix C. The summary has been based on [Malt], [Boll], [Wood] and [Sand].

Fingerprint features and classification

As described in the summarized history of fingerprints above, there have been different attempts to classify fingerprints for manual matching. During the years of working with fingerprint matching, examiners have come to a point to discuss three levels of detail in fingerprints [Wood] and [Malt].

- Level 1, the global level, or the Galton level: Have a look at your fingerprint. You can see it is a "landscape" full of papillary lines. The higher and lower parts of the papillary lines are called ridges and valleys respectively. According to Harris [Harr] the formation of these ridges and valleys are a combination of several environmental and genetic factors. The directions in the skin formation is given in the DNA structure, but the final structure of the fingerprint is formed by different random events such as the position of the foetus in the womb, and the composition and density of surrounding amniotic fluid. This is why fingerprints, unlike DNA, are different on identical twins [Sand]. The flow of the ridges and valleys, together with the singular points, core and delta (see Figure 4), ridge count and orientation, all belong to the set of features that can classify and index a fingerprint at the first level. The patterns are classified using the Henry classification system. For more background on this system, see Appendix C - Fingerprint History.

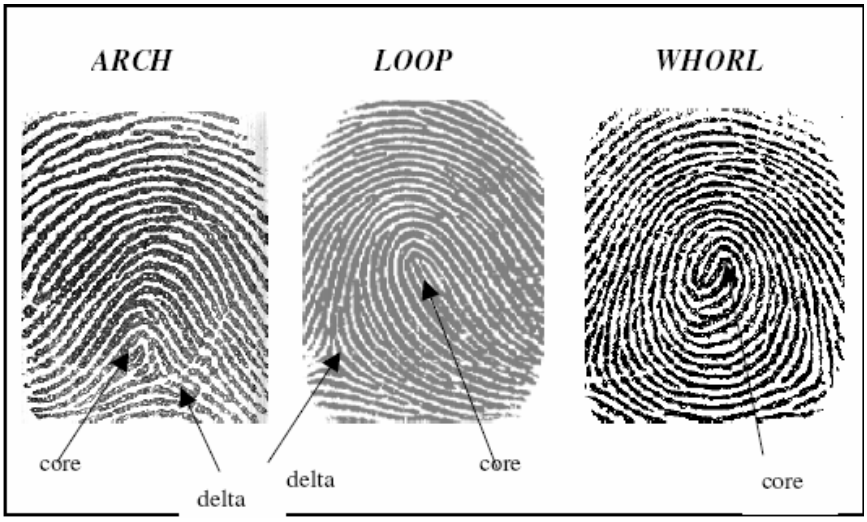


Figure 4: Fingerprint patterns: arch, loop, and whorl. Fingerprint landmarks are also shown: core and delta. (No delta locations fall within the captured area of the whorl here.) Source [Boll].

- Level 2, the local level: At the local level the examination process looks closer at different local ridge characteristics, so called minutiae. A minutiae characteristic is either a ridge termination, where a ridged ends, or a ridge bifurcation, where a ridge diverges into two new branch ridges. The NIST Standard for Forensic Identification definition on minutiae is: "Friction ridge characteristics that are used to individualize that print. Minutiae occur at points where a single friction ridge deviates from an uninterrupted flow. Deviation may take the form of ending, division, or immediate origination and termination" (ANSI Glossary 1988 from [Wood]). Other changes on the ridges might be: islands, dots, independent ridges, lakes, spurs and crossovers. Figure 5 illustrates typical minutiae characteristics (red points) on a fingerprint.

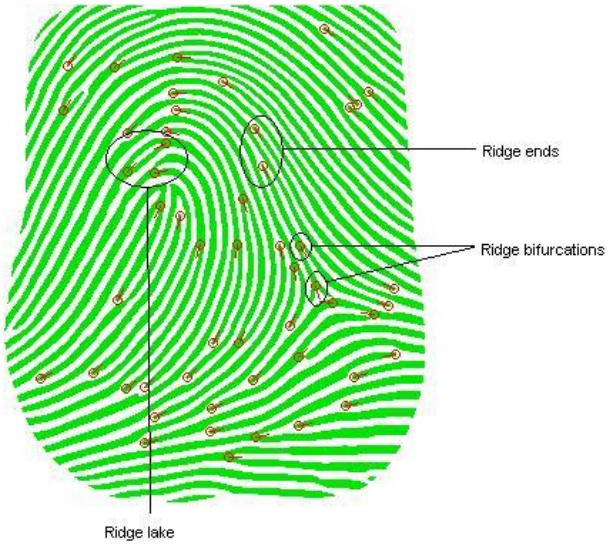


Figure 5: Examples of ridge characteristics in a fingerprint. Fingerprint captured with a digitalpersona U.are.U® 4000 Sensor and Verifinger Demo Software [Neur].

- Level 3, the very fine level: At this level, intra-ridge details can be detected. These are essentially the shape and position of the sweat pores which are considered highly distinctive and can help identify a person. However, to be able to view this information, a high resolution image of the fingerprint is required [Malt]. Sweat pores can be viewed as small dots on the ridges in Figure 6.

Figure 6: A fingerprint image with minutiae details and sweat pores visible. Fingerprint captured with a digitalpersona U.are.U® 4000 Sensor [Digi] and Verifinger Demo Software [Neur].

Fingerprint matching is one of the most widely used characteristic for biometric

authentication, and therefore also one of the leading technologies [Web25]. This might be because fingerprint authentication meets most of the following requirements (for descriptions of the different terms, see Chapter 4); universality, distinctiveness, permanence, collectability, performance, acceptability, circumvention, reliability, ease of use, ease of implementation, and low cost. However fingerprint authentication also meets some potential problems.

- Presentation of fingerprint. The presented finger will most likely be in a different location than the original image(s).
- The presented finger might also have a different orientation, for example upside-down.
- Skin elasticity. Even if the finger is in right location and with the right orientation it might not be recognized because of the elasticity of the skin.
- Pressure. Pressing the finger to hard or to soft on the sensor might cause differences in location of all features.
- Bad quality of fingerprint images both enrolled and presented. To help this, Putte suggests that the finger should be scanned at least "three to four times to get a profile that is independent of variations that occur in practice, such as the angle of placement of the finger on the scanner" [Putt].
- Essential minutiae might be missing in the captured image.
- Other noise such as thicker or thinner ridges, discontinuities of ridges, dry/oily finger, cold finger, cuts or bruises causes differences on two images.
- Impostor attacks. There have been several successful attempts to fool a fingerprint recognition device. Information and discussion of this topic can be further explored in [Putt], [Sand], [Blom] and [Mats]. A good way to improve the security is to use a liveness detection system, which can determine if the presented fingerprint is a part of a living body or not [Sand], but these systems are also possible to fool. More information and discussion on this topic can be found in [Sand] and [Wood].

3.3.2 Eye biometrics: Iris and Retina

Two of the most accurate biometrics lies in the eye, the iris and the retina [Wood].

Iris scanning

The iris is located in the front of the eye. It is the colored ring around the pupil, and has muscles that adjust the amount of light entering the eye. In addition to expand the iris allowing less light entering the eye, and constrict the iris allowing more light enter the eye, these muscles are affected by internal physiological responses and thus constrict or enlarge the iris. The iris is composed of many different features, such as ridges and

furrows, rings, crypts, a corona, and sometimes freckles [Boll]. Iris color is usually not one of these features since iris images often are captured with monochrome cameras using infrared lights. Figure 7 shows an example of an iris pattern.

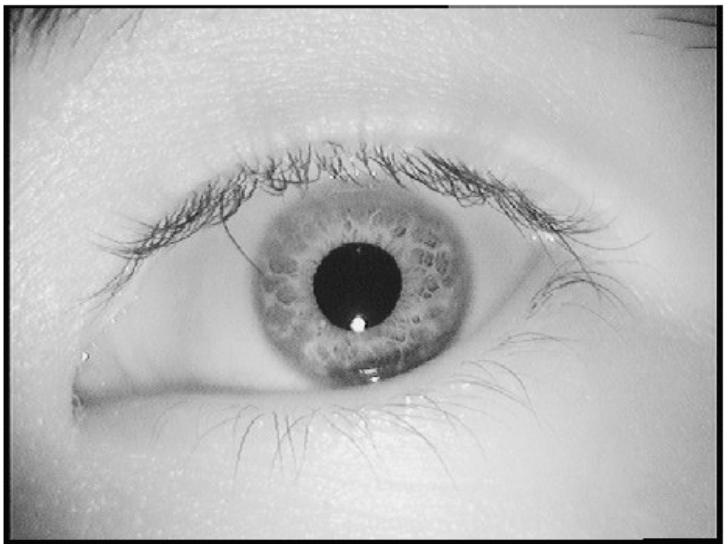


Figure 7: An iris pattern scanned with infrared light [Boll].

According to [Wood], studies have shown that no two irises are identical. Not even the left and right iris on the same person. The iris has no known genetic dependencies, is formed from birth, and under normal health conditions remains stable until death, which makes it ideal for biometric authentication. However, some diseases can affect and alter the structure of the iris. Iris melanoma is such a disease, but it is very rare. Of course since the eye is a very sensitive organ, other injuries can also occur.

A drawback with iris scanning is that it cannot be used to identify a person at a distance, no more than 5 meters. The usual distance commercial iris scanners work at is 3 to 7 inches. An iris authentication can briefly be described as: An image is taken, scanned and processed in grayscale values. The iris is then located and isolated in the image, and size and contrast corrections are performed to achieve a size-invariant representation [Wood]. The detailed iris pattern is then encoded and represented by a 256-byte 'Iris Code'. Two iris images are compared by using XOR operations on all bits. The difference is then the number of mismatched bits, also called Hamming Distance (HD). Dr. J. Daugman has performed a mathematical analysis of IrisCode comparisons, and found that they have a very low error rate. With a HD criterion of 0.342, the chance for a false accepts is 1 in 1.2 million [Boll].

This means that iris recognition is very accurate, and is therefore more and more used as an authentication method. However, it is important to know that iris recognition also has some drawbacks. (Some of these are mentioned earlier). The accuracy depends

heavily on the application and intended use.

Retina scanning

The retina contains small blood vessels which lay in a special pattern in the back of the eye. This biometric feature is perceived as the most secure authentication method, and is often used in high-security environments such as nuclear research and weapon sites [Boll]. Figure 8 shows the location of the retina, and how it captures the light. A study performed by Dr. Paul Tower, described in [Boll], showed that among the biometric factors compared between two twins, retina patterns were least identical. The retina is also more stable than other biometrics, since it is not exposed to external environments, such as fingerprints or a face. It also remains unchanged throughout life [Wood]. However, eye injuries, severe damage to the eye, and different diseases can cause deformations, and can alter the retina.

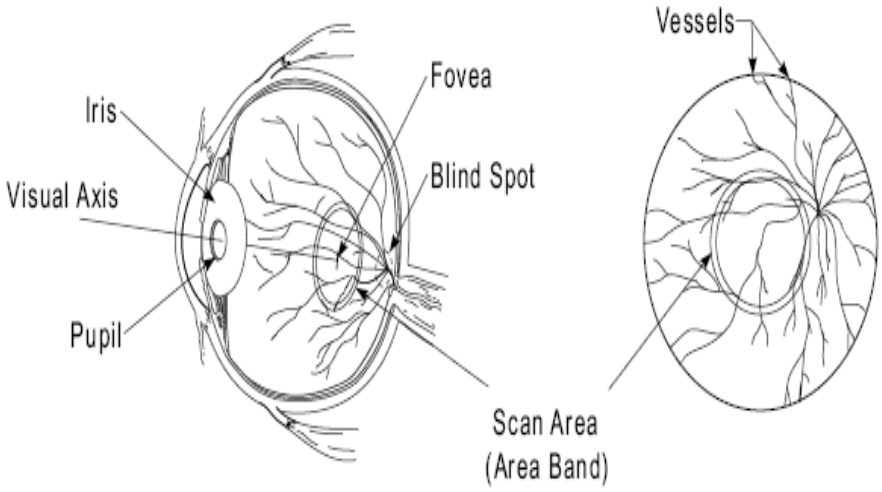


Figure 8: Eye and scan circle, [Boll].

To perform a retinal scanning, the retina is illuminated with a low-intensity infrared light so the patterns of the major blood vessels can be scanned. Because of the location of the retina, retinal scanning relies on the users to cooperate. The scanner normally requires that the user is in a distance of 2 to 3 inches. This makes it impossible to use for example for surveillance. Some also allege that it is inconvenient in use, and despite its high quality on results, is likely to being more cumbersome than for example fingerprint recognition. Retina scanning is also of the more expensive biometric systems, but more convenient and inexpensive scanners are coming to market.

Because of the high accuracy of retina scanning, false acceptance rates for this technique are close to zero, and false rejections that occur are often connected to user unfamiliarity. Retina scanning, together with iris scanning are thought to be two of the better methods for biometric authentication. Both have strengths in that they are very accurate, and cannot so be easily copied. The retina is more protected than the iris, but the technology is also more expensive. As with all other biometrics, cost, initial costs, installation and integration, along with accuracy and user preference must be weighted when choosing an eye biometric system.

3.3.3 Hand geometry

Hand geometry is the second most biometric characteristic widely used for biometric authentication [Wood]. The idea is that the shape and features of the hand can be used to correctly identify a person. As with fingerprints, each human hand is unique. This is because of the length, width, thickness, and curvatures of the finger and the hand, and the relative location of these features [Boll]. Figure 9 shows how hand geometrics are measured.

Hand geometry can be used in situations where the identity of a user needs to be verified. It's however, not good enough to do an identification search [Wood], [Boll]. In an environment where privacy issues are concerned, this might therefore be a better solution than, say for example fingerprints, because the characteristics is, according to Woodward et al., not good enough to identify a match in a large database of stored templates.

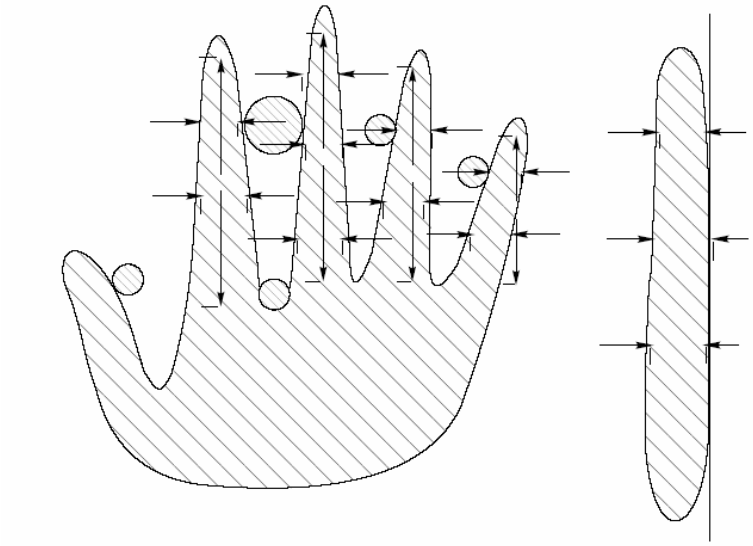


Figure 9: Typical measurement of hand geometry [Boll].

3.3.4 Face recognition

Face recognition is, as the name implies, authentication of a person based on different characteristics in his or her face. Humans often recognize each other by their faces, but no one knows which are the most significant characteristics used when a human recognizes another humans face. This is the reason why there is no unified theory on how to best represent and recognize a face in an automated biometric authentication system. However the fundamental structure of the face is mostly used and most systems are invariant to variables like position, pose, expression, facial hair or glasses.

Face recognition software can operate in different environments, from well controlled environments to uncontrolled environments. An example of a controlled environment is when a person sits in front of the camera, and is looking straight into the camera without any special expressions. This method is usually used for verification (see Chapter 2.1.2). An example on an uncontrolled environment could be a surveillance camera at a football match, scanning the faces of the crowd, looking for known hooligans. This method is usually used for identification (see Chapter 2.1.1).

It is easy to understand that the face recognition technology has some challenges. The first thing in a face authentication process is the detection of a face. A face is detected according to shapes and features in the image, such as eyes, ears and mouth. A problem is that the face can be in a different position than the enrolled image. This can make it more difficult to identify. Background is also a challenge, and hence it is also important with a background removal feature, to remove noise and make the image as ideal as possible.

To cope with some of the problems, neural networks is often used in face recognition software. This allows the software to 'learn' how to perform classification tasks based directly on patterns in data [Wood].

Face recognition software is less accurate than for example eye biometrics and fingerprints, and the decision to make it the primary biometric technique in the new biometric passports has been heavily criticized [BTT]. In FRVT 2002 (Facial Recognition Vendor Test 2002) the most accurate face systems displayed a 71.5% true acceptance rate at a 0.01% false acceptance rate, and 90.3% true acceptance rate at 1.0% false acceptance rate (verification)[FRVT].

This makes it not very usable in high security environments, but since the technology is inexpensive, acquires little involvement from the user, and hence makes it ideal for surveillance, it is very popular in other settings.

3.4 Behavioral biometrics

[Web8] provides the following definition on behavioral biometrics: "Behavioral characteristics are based on an action taken by a person. Behavioral biometrics, in turn, are based on measurements and data derived from an action, and indirectly measure characteristics of the human body". Behavioral biometric characteristics are in literature also denoted as an alterable biometric signal. This is because the captured "biometric signal" is a combination of two components, the underlying, stable biometric, and a variable which for example can be a word or phrase, speed, terrain, text etc [Gorm]. Examples of behavioral biometrics are voice recognition, keystroke-dynamics, and signature-dynamics. An easy way to find out which category a biometric signal should belong to is to use time as a metric to decide whether a biometric characteristic is physiological or behavioral. If the sample has a beginning, middle and end it is behavioral.

3.4.1 Voice recognition and voice verification

Voice recognition is a very common biometric technology. "The goal of voice recognition is to understand spoken words and sentences – that is, the content of what is being said" [Wood]. The voice recognition technology will be valuable in systems that require hands free systems, such as hand free sets for mobile phones and voice command interpretation in automated telephone call centers. Other potential uses include computers, cars, consumer electronics, and even appliances [Wood].

Voice verification, concentrates on identifying who is speaking. This is done by comparing an individual's voice sample with the user's previously enrolled sample of the same utterance. The utterance can be a short word or phrase. Speaker verification, speaker authentication, voice authentication, talker authentication, and talker verification are different terms for voice verification [Boll]. One can say that voice verification (speaker recognition) is a biometric characteristic with both physiological and behavioral components. The physical shape of the vocal tract, which consists of the oral and nasal airways, and the soft tissue air cavities, are the primary physiological components. The speech production is controlled by these components along with movement of mouth, jaw, tongue, pharynx, and larynx. The behavioral aspects of voice verification are formed by the motion, manner, and pronunciation of the words [Wood].

There are two modes which voice verification can operate in. Most common is the constrained mode, or text-dependent mode, where the user is restricted to predetermined single words or short phrases. In unconstrained verification mode where the speech input is free, or text-independent, the user is not required to say the same sentence during each access, but this mode has a higher error rate than the constrained mode [Wood].

Typical factors that can contribute to authentication errors are:

- Age: The vocal tract and thereby the voice pattern can change over the years
- Sickness: Colds can alter the vocal tract and thereby the voice pattern
- Acoustics: Samples can vary if they are provided in different environments, e.g. if the individual has to speak louder due to noise
- Misread or misspoken utterances, words or phrases
- Emotional states of individual, e.g. stress or duress
- Placement of or distance to microphone, or the use of different microphones
-

However, voice verification provides valuable information for authentication purposes, but is not robust enough to determine an identity by itself, much because it is so vulnerable especially to tape recorders and mimicry by humans [Malt].

3.4.2 Signature dynamics

Signature dynamics is, as the term implies, how a personal signature is generated, and what features it holds. Geometry, curvature, and shape information of words and characters are all features provided by the signature itself, while pressure metrics, stroke direction, speed, and pen up and pen down events says something about how the signature was generated [Wood].

Signature verification can be divided into two groups [Boll];

- Off-line signature verification: Signatures who only have a static visual record, such as Signatures on traditional paper, paintings etc, often written with ink.
- On-line signature verification, or digitized signature verification: Signatures where pen trajectory and/or dynamics are captured by an electronic device and digitized.
-

Transformation and atomization of off-line signatures to digitized media is a complex process, and hence a reliable verification of these signatures is not possible. The verification of on-line signatures is on the other hand very feasible, and is more and more used for authentication in the business world. Although signature dynamics is often used for authentication, it has some weaknesses or limitations. It is mostly used for one-to-one verification, and there exists no basis research for claiming that signatures are as individual as for example DNA, which means that it might be possible that two or more individuals have similar signatures. Also, different signatures collected from the same person might vary in shape and features. Other weaknesses can be the shape and weight of the pen, the surface on which the signature is written, personal and emotional factors at the time of the signing, and if the signing is routine or not. For

example a person might be more relaxed signing routine papers than signing important contracts, and hence the speed, pressure, etc might be different. For more on signature dynamics, see [Wood], [Cran], [Plam], [Boll].

3.4.3 Keystroke dynamics

The idea of keystroke dynamics is to identify a user "based on his/her typing technique using traditional pattern recognition and neural network techniques" [Boll]. One of the advantages with keystroke dynamics compared to signature dynamics (see Chapter 5.2.2) is that no additional equipment is required. The capturing of keystroke dynamics lies entirely in the software, which means that it can be integrated into most computer systems.

Keystroke dynamics recognition systems can either be used for single authentication, or for continuous monitoring. For single authentication the user typically is required to type a phrase as he/she normally would do, and the software compares this provided template with the one previously stored for this user. In a continuously monitoring system, the software monitors the keystroke dynamics detected on the keyboard. If a user for example left his working station unattended and another person started using the computer (typing on the keyboard), the system could immediately recognize this as a different user, lock the system, and ask for re-authentication.

One of the purposes of using keystroke dynamics for authentication is to make passwords more secure. Because keystroke dynamics require the user to type the password in a certain way, with regard to speed, hold time, press and release pattern etc, it will be more difficult for an impostor to falsely authenticate to the system, even if he/she knows the password.

One of the disadvantages that might follow keystroke dynamics is that users might not accept it because they feel that it records too much information about them. Keystroke monitoring is also sometimes known as spyware, which can be used to for eavesdropping others. Information that can be revealed by keystroke dynamics software are; passwords, emails, work (such as important research), private chat sessions, and other things that are written when a user presses the keys on a keyboard. For more on keystroke dynamics, see [Wood], [Obai], [Umph], [Boll].

3.5 Esoteric biometrics

3.5.1 Facial thermography

The idea of facial thermography biometric recognition uses cameras sensitive in the infrared spectrum to recognize patterns of facial heat. The facial heat (see Figure 10) is caused by the blood flow under the skin, and makes a distinct pattern. Facial thermograms yield the same blood vessel pathways that are the underlying vein and

tissue structures, but the dynamic nature of blood flow causes fluctuations due to environmental conditions such as variation in temperature, ingestion of alcohol, drugs and cigarette smoke.

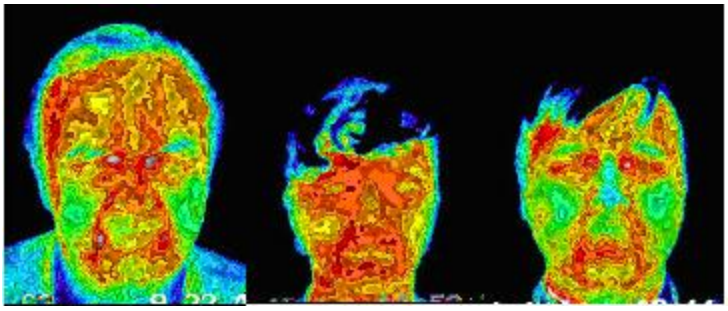


Figure 10: Infrared face images of three individuals, [Boll].

Facial thermography has a special feature that other biometric characteristics cannot provide, the image can tell if the person is present or absent, alive or dead, attentive or inattentive, physically rested or fatigued, relaxed or anxious [Wood]. This is one of the reasons facial thermography has not evolved much. User acceptance is very low, since it is possible to reveal information about someone's health situation. This is clearly a drawback, but it can also be used as an advantage in situations where it is needed to confirm the medical condition of a person, for example if a person has been suspected for driving under the influence of drugs or alcohol, or to see if a surgeon or flight traffic controller lacks rest.

There are also some other advantages/disadvantages of this biometric technique [Wood]:

- It works in the dark, and can therefore have a better recognition rate in situations where it is complete darkness, or with light coming from a different angle, which is a problem for face recognition cameras.
- It is possible to take images of persons unaware of the situation, making it ideal for surveillance.
- Cameras are often expensive, and the technology a bit more complicated than most other regular biometric techniques.
- Image resolution is lower, and there is more noise in the thermal image.
-

It is suggested that facial thermography should complement face recognition systems because it provides additional information, as well as liveness testing which makes it harder for an impostor to use a mask or similar for authentication. For more on facial thermography, see [Boll], [Chel] and [Wood]

3.5.2 DNA

DNA is the acronym for deoxyribonucleic acid. [Web21] describes DNA: "DNA molecules carry the genetic information necessary for the organization and functioning of most living cells and control the inheritance of characteristics". A May 2002 whitepaper of the Australian Institute of Criminology explains (cited in [Wood]):

> "The DNA in a human cell is unique, the product of sexual reproduction that combines half of the mother's DNA and half of the father's DNA. Every cell in an individual's body is the result of cellular division, which copies the DNA in the newly fertilized cell into every other nucleic cell. As a result, DNA in a cellular nucleus is identical throughout a human body but variable between any two humans, making it a natural alternative to artificial human identifiers, such as names or tax-file number. The notable exception is identical twins, which develop from a single fertilized cell and hence have identical nuclear DNA".

DNA is a way of biometric characteristic, but differs from standard biometric characteristics in several ways [Web22]:

- DNA requires a tangible physical sample as opposed to an impression, image, or recording.
- DNA matching is not done in real-time, and currently not all stages of comparison are automated.
- DNA matching does not employ templates or feature extraction, but rather represents the comparison of actual samples.
-

There is also a concern about contamination and sensitivity: It is easy for anyone to steal a piece of DNA from an unsuspecting person that can be subsequently abused for an ulterior purpose. And there are of course privacy issues because "information about susceptibilities of a person to certain diseases could be gained from the DNA pattern and there is a concern that the unintended abuse of genetic code information may result in discrimination, e.g. in hiring practices" [Gorm], [Malt].

Because of this, DNA is not used in other than forensic applications. Example of this might be in a homicide case, when a DNA structure different from the victim's is found at the murder scene. If the investigators have one or more suspects, their goal is to match the DNA left on the murder scene with the DNA of one of the suspects. Alternatively, the goal could be to match the DNA of the victim with one found on the suspect's personal effects, such as hair, clothes, shoes etc. To protect individual privacy only parts of the DNA that functions are not known, or not is in the part that produces a detectable effect, are used for law enforcement and forensic purposes [Wood].

The acceptance of DNA has made it possible to establish databases of DNA samples, for

example the Combined DNA Index System (CODIS) that enables federal, state, and local crime labs to exchange and compare DNA profiles electronically [Wood]. It is therefore possible to match profiles across borders, and DNA has the advantage of being distinctive (except for identical twins) and it does not change over the lifetime of an individual. However, there are some challenges; DNA testing cannot, at present, be done in real-time, although research in this field is underway to create products that will cut the processing time dramatically. There is also a concern of acceptance issues. Because DNA provides such a wealth of data, it "might be considered overkill for the purpose of authentication in normal daily activities" [Wood]. For more on DNA, see [Wood], [Boll], [Inma] and [Kirb].

3.5.3 Vein pattern recognition

The idea of vein pattern biometric recognition relies on using a special camera together with an infrared light. The camera captures images of the vascular pattern made by the blood vessels everyone has on the back of their hands. These patterns are developed at the foetus stage, differ even between identical twins, and are, except from their overall size, consistent throughout life.

There has not been much research on vein pattern recognition, but the biometric characteristic certainly has some advantages and disadvantages [Wood]:

- It is nearly universal because most people are in possession of it.
- The veins are not so exposed to damage since they are covered by the skin, and they are not so easy to alter or copy (at least not with the techniques used today).
- It also seems to satisfy requirements for distinctiveness, permanence and collectability.
- It is uncertain whether drugs, exercise, mental health and medical conditions affect the blood flow and thereby the vein patterns.
- Because of the infrared light, vein pattern recognition is more expensive and complex than other biometric techniques.
-

It is suggested that vein pattern recognition should not compete with the other biometric techniques to be used as a single technique for authentication. Much of the research on vein pattern recognition suggests that the technology should instead complement other techniques in a multimodal biometric authentication system.

3.6 Biometric authentication systems in summary

As biometric authentication systems become embedded into more and more systems (e.g. cellular phones, keyboards etc), [Malt] believes it is important "to analyze the impact of biometrics on the overall integrity of the system and its social acceptability as well as the related security and privacy issues".

It is not possible to decide which biometric techniques is "the best", [Web19], The International biometric group has developed a model illustrating how the different biometric technologies differ from the "ideal" biometric, Figure 11. In this analysis they compare the different biometric technologies in terms of ease-of-use, cost, accuracy, and perceived intrusiveness.

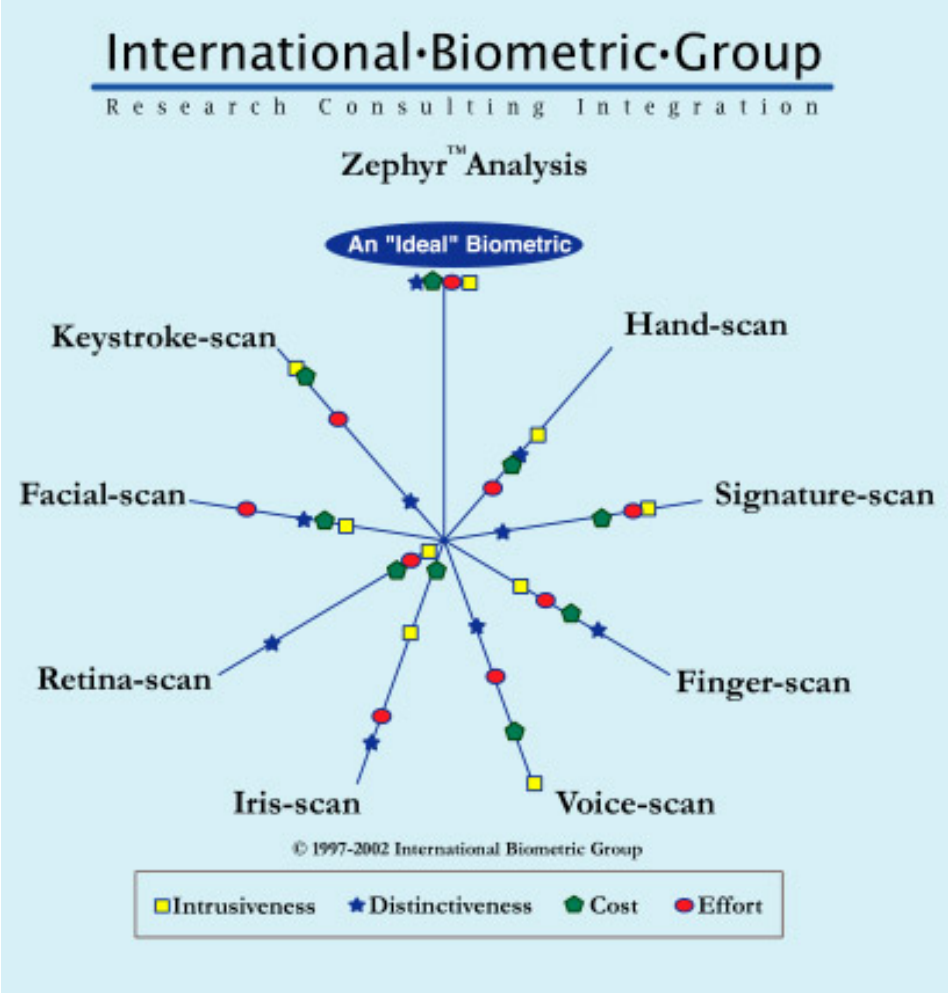


Figure 11: Comparison of different biometric technologies. [Web19].

The symbols in the illustration represent the relative capabilities of each technology, where a perfect system would have all the values at the periphery. A system with values near the centre of the figure is a poor biometric system. Another approach to find the strengths and weaknesses for the different biometric technologies has been done by [Malt]. As it is possible to read from the figure, most of the techniques have their different strengths and weaknesses. For example a voice scan scores very high on intrusiveness, but lower on distinctiveness, while a retina scan scores almost the opposite on these two factors. One of the techniques with no specific weak or strong point is the finger scan. This is one of the reasons why fingerprint scan has been chosen in this study.

Table 3 illustrates how Maltoni et. al. rate the different techniques when it comes to universality, distinctiveness, permanence, collectability, performance, acceptability, and circumvention. The data are based of the perception of the authors (Table from [Malt] – handbook of fingerprint recognition, p 12). The levels are: High, Medium, and Low, and are denoted by H, M, and L, respectively. A high level in e.g. universality means that the biometric identifier is likely to be universal between two individuals. A biometric identifier with most H's is likely to be a better identifier than an identifier with mostly L's, depending on the situation.

Biometric identifier	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
DNA	H	H	H	L	H	L	L
Ear	M	M	H	M	M	H	M
Face	H	L	M	H	L	H	H
Facial thermogram	H	H	L	H	M	H	L
Fingerprint	M	H	H	M	H	M	M
Gait	M	L	L	H	L	H	M
Hand geometry	M	M	M	H	M	M	M
Hand vein	M	M	M	M	M	M	L
Iris	H	H	H	M	H	L	L
Keystroke	L	L	L	M	L	M	M
Odor	H	H	H	M	H	L	L
Retina	H	H	M	L	H	L	L
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

Table 3: Comparison of biometric technologies.

4 Implementation of methods in survey

As mentioned in Chapter 1.5, the method used in this study is in literature referred to as a mixed method approach. A mixed method approach is a combination qualitative- and quantitative research methods, and makes use of these two methods when collecting and analyzing data [Cres]. The qualitative method has been used in the literature study while the quantitative method has been used in the survey to analyze the results.

4.1 Procedure of the experiment

Two sessions were appointed to each participant. At the first session they got an introduction to the experiment similar to the information letter and letter of agreement, see Appendix B. All participants also got a demonstration of a biometric authentication system, represented by a fingerprint capture device (digitalpersona U.are.U® 4000 Sensor [digi]) and a software for handling digitalized fingerprints (Verifinger Demo Software [Neur]). This demonstration showed the participants how a fingerprint can be used instead of password for authentication on a computer. After the demonstration the participants enrolled in the Verifinger software. The enrolment procedure captured three images of the left thumb of the participants, and made a profile with a number as username, and the three images as a base for authentication. After the enrolment a mould of each participant's fingerprint was made in a lump of clay. This lump was later used to make a copy of the fingerprint, see Chapter 4.4. At the end of the first session, the participants were asked to complete the first questionnaire. Any questions or contributions were also discussed. The participants were informed that they should not consider what might be the more correct answer in the questionnaire, but rather give their own opinion.

Between the two sessions, the author made the artificial fingerprint as it is described in Chapter 4.4. One of the participants did not allow a copy being made, so the mould of this participant was brought back unprocessed. Another participant did not return the letter of agreement, so the mould of this participant was also brought back unprocessed. To demonstrate how an artificial fingerprint can be used to fool a fingerprint recognition system, an artificial fingerprint from the author was made. This was used in the situations where the artificial fingerprint from the participant was of such bad quality that it did not work for authentication.

The artificial fingerprints were brought back for the second session and used to demonstrate a log in session from an impostor. See Figure 12 for images of a fingerprint from a real finger versus the fingerprint of the artificial finger. A successful login was

registered with 15 of the artificial fingerprints, while the other 15 were not successful. Idealistic all the artificial fingerprints should be successful so each participant would see that their fingerprint could be used by an impostor. However, with a useable copy of the fingerprint of the author, these participants also saw a demonstration of an impostor attack. At the end of the second session, the participants were asked to complete the second questionnaire. Any questions or contributions were also discussed. The participants were, as in session one, informed that they should not consider what might be right or wrong in the questionnaire, but rather give their own opinion.

When the answers from the second questionnaire were returned, the data were entered into a Microsoft Office Excel worksheet, and analyzed. The analysis is performed, and the results are discussed in Chapter 6.

Figure 12: Images captured from the experiment. Fingerprint of a real finger, to the left, and fingerprint of the artificial finger, to the right.

4.2 The participants

Forty-eight employees from 'Sykehuset Innlandet, Gjøvik' were asked to participate in the study. Three of the employees did not attend to or did not hand in the answers from the first survey, and another nine employees did not attend to or did not hand in the answers from the second survey. Four of the surveys were incomplete, and hence these surveys were also removed from the results. This gave a total of thirty participants completing the whole study (both surveys). Seven of them were men, and twenty-three were women. The age ranged from 20 to 50+. Five of the participants had studied IT.

The participants represented two departments; the radiography department with 22 participants, and the laboratory department with 8 participants. First-time contact with was made through Kai Kristiansen, the contact for the project at the hospital. Børge Sandstedt and Anne Grethe Mathisen also helped coordinating the participants.

4.3 The system

The system used in the experiment is quite simple. It consists of a fingerprint sensor, fingerprint authentication software, and a computer. In this case the digitalpersona U.are.U® 4000 Sensor which uses a USB connection was chosen as a sensor, the Verifinger Demo Software from Neurotechnologija was chosen as software, and a Toshiba® Satellite Pro M30 personal laptop running Windows XP was chosen as laptop. The laptop was set up with the following specifications: Intel® Pentium® 1,79GHz processor and 512 MB RAM. The software worked well on the laptop with these specifications, but would probably work with lower specifications as well (no experience). Figure 13 shows how the system was set up. Left is the digitalpersona U.are.U® 4000 Sensor, in the middle the laptop with the Verifinger Demo Software running, down bottom an example of a fingerprint mould in a lump of clay (left), and an example of an artificial fingerprint (right).

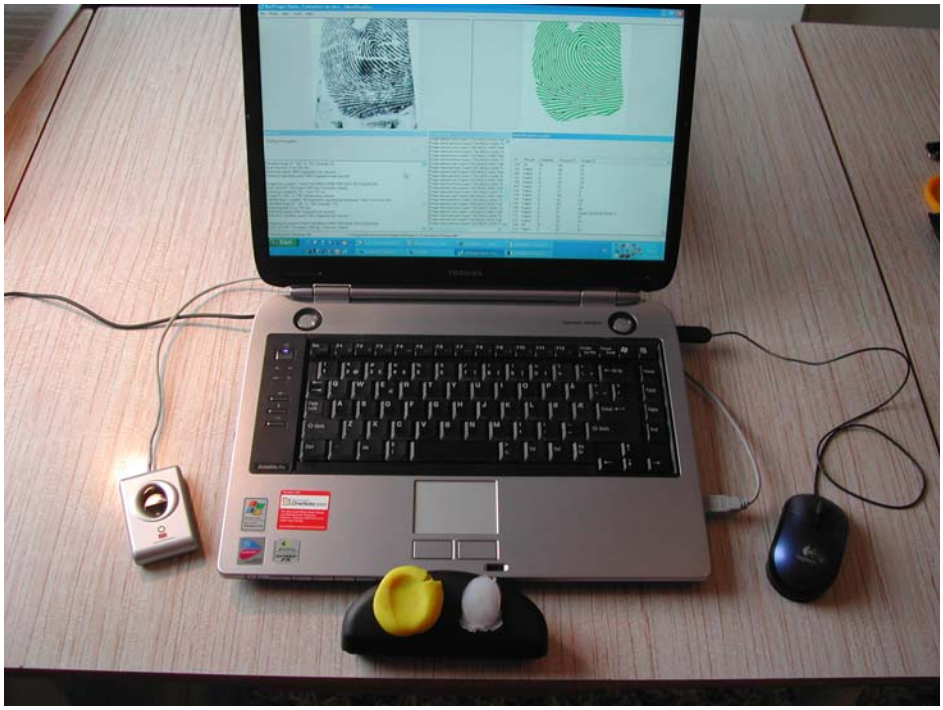


Figure 13: Set up of the experiment.

4.4 Making of the artificial fingerprint

The method used to create artificial fingerprints in this study is inspired by Ton van der Putte & Jeoren Keuning [Putt], Johan Blommè [Blom], Marie Sandstöm [Sand], and T. Matsumoto et al.'s [Mats] experiments. In this experiment a mold was made of the real fingers from the participants, and a silicone solution was used to fill the mold to create the artificial fingerprints.

4.4.1 Mold

In their experiments, Matsumoto et al. used a sort of molding plastic named 'Freeplastic' [Mats], while Blommè used 'Siligum – Silicone moulding paste' [Blom]. None of these were available for purchase for this experiment so a different material has been used.

4.4.2 Making of the mold

Important factors when choosing material for the fingerprint mould was:

- To find a material which was usable, so a decent fingerprint could be left in the material
- To have the possibility of making around 50 fingerprints at the same time
- To find a material which not was too expensive
- No need of reuse of the mold for additional fingerprints since only one fingerprint is needed for each participant
- The mould should be easy to destroy after use
-

Because of these requirements, a type of play clay for children, 'Play Do'h' was chosen. This type of clay is soft enough to make a good mold of the fingerprint, it is possible to make several clay-molds at low-cost, and it is difficult to produce two fingerprints from the same mold, which protect the participants' privacy issues.

The lump of clay was rolled like a ball for a few seconds so the clay softened. Then the mold could be made by pressing the tip of the finger gently against the clay so it formed around the finger. The finger did not have to be in contact with the clay for more than a few seconds since the material already was solid. It was important, however, to press the finger slowly, and not move it to the sides during the making of the mold. This is because too much movement of the finger could cause the mold to become different in shape and size so that unwanted patterns, such as wrinkles and scars, and important features, such as minutiae could appear in another way than in the original fingerprint. Bubbles of air could also make the mold unusable. It was therefore important to examine the mold after the finger was removed and make a new mold if the first one seemed to be of bad quality. Figure 14 shows, to the left, how the clay appeared after the finger created the mold, but before the artificial finger was made.

4.4.3 Artificial fingers

When choosing method for making an artificial fingerprint, it was important to know what type of fingerprint sensor was going to be used because different types of sensors react differently to different types of artificial fingers. For more on fingerprint scanners, see [Blom]. Other factors that should be considered were; permeability, humidity and solidity [Blom]. If given enough time, it is possible to choose from a wide variety of different materials, such as gelatin, glue, and silicone, to optimize the artificial fingers, to maximize the number of acceptances of the false fingers, or FAR (see Chapter 2.3.1).

The sensor in this experiment was optic and one of the best materials for creating an artificial finger to fool an optic sensor is silicone. The reason why silicone is more suitable than gelatin when using an optic sensor might be because gelatin is quite transparent, while silicone is "opaque and the texture of the right kind of silicone resemble skin at an acceptable level" [Blom].

Because of this, a regular type of glass silicone was chosen in this experiment.

4.4.4 Making of artificial finger

Making the artificial fingerprints with the silicone solution was quite simple, but it was important to avoid bubbles. The silicone came in a tube, and was smeared onto the mold. To avoid bubbles up to a point, and to cover the whole fingerprint, the silicone was smeared out onto the mold by using the finger of the author. (It is recommended to use some sort of glove to protect the skin from the silicone which can be very "sticky"). To avoid breaking the artificial finger when the silicone was removed from the mold, the silicone stayed in the mold a couple of days before it was removed. When removing the silicone finger from the mold of clay, depending on the consistence of the clay, some clay might attach to the artificial fingerprint. This clay can easily be removed by gently rubbing it off with a wet piece of cloth or simply your own finger. After the silicone finger was removed from the mold, the artificial fingerprint was used to attempt to fool the fingerprint sensor. Figure 14, to the right, shows an example of a silicon finger after it has been removed from the mold. Due to privacy issues it is important to make sure the mold can not be used a second time. To be sure this is not possible the clay ought to be squeezed together.

Figure 14: Fingerprint mould in a lump of clay and an artificial fingerprint made of Silicone.

4.4.5 Privacy issues

Since the experiment handled sensitive information it had to be reported to the Norwegian Social Science Data Services (in Norwegian: Norsk Samfunnsvitenskaplig Datatjeneste (NSD)). A standard form for reporting is available at their homepage [NSD]. For this project, the approval can be found on their webpage. Apart from the fingerprints, no other information was regarded as sensitive in a way that a single person can be recognized based on his or her answers, so the survey will not come in conflict with other privacy issues.

The silicone finger containing the artificial fingerprint was not removed from the mold, without the participant present. After the silicone finger had been used for the experiment, this was given to the participant with recommendations to destroy it. They also saw the mold which was used to make a copy of their fingerprint being destroyed. By doing this the participant can be sure that their fingerprint provided in this experiment will not be used by others at a later time.

5 Presentation of results

The overall results from the survey are presented in Table 4.The same questionnaire was used for both sessions, so that any differences between the sessions could be discovered and analyzed. The questionnaire can be found in Appendix A. Nine participants did not finish the second survey, and five participants did not fully answer one of the questionnaires. These answers were therefore omitted from the results, which gave a total of 30 complete sets of questionnaires to use in the analysis.

The answers from the second questionnaire are in brackets ().

#	Question	Categories of answer and total number of answers
2	Sex	Men: 7 (7) Women: 23 (23) Total of 44 (35)
3	Age	16 -20: 0 (0) 21 -30: 6 (6) 31 -40: 6 (5) 41 -50: 9 (10) 50+: 9 (9)
4	Department	Radiography: 22 (22) Laboratory: 8 (8)
5	Have you ever studied IT?	Yes: 5* (5) No: 25 (25) Don't know/remember: 0 (0) *only short courses, 2 years is highest
6	At what level do you feel you are when it comes to knowledge and usage of IT?	Very high: 2 (2) High: 8 (5)

		Neither	13 (18)	
		Low	5 (4)	
		Very low	2 (1)	
7	How often do you use computers in daily work?	Several times a day	30 (30)	
		Once a day	0 (0)	
		1-3 times a week	0 (0)	
		1-3 times a month	0 (0)	
		Seldom or never	0 (0)	
8	Do you authenticate when logging onto a computer?	Yes	30 (30)	
		No	0 (0)	
		Don't use computers	0 (0)	
9	Have you ever lend out your ID-card or told your password to anyone?	Yes	21 (22)	
		No	9 (8)	
		Don't remember/Don't want to answer	0 (0)	
10	Have you heard about biometric authentication before this experiment?	Yes	24(24)	
		No	6(6)	
11	Have you ever provided biometric information for use for authentication in any sort of situation?	Yes	3 (8**)	
		No	27 (22)	
		**This number has probably risen because some of the participants include the first session of this experiment		
12	Have you ever used any of these biometric techniques to authenticate?	Eye	0 (0)	
		Fingerprint	0 (1)	
		Face recognition	0 (0)	
		Voice recognition	1 (0)	
		Hand geometry	0 (0)	

		Signature	7 (10)

13	How comfortable are you of registration and use of your biometric information?	Eye (iris/retina)		Fingerprint	
		Very comfortable	9 (11)	Very comfortable	12 (7)
		Somewhat comfortable	13 (8)	Somewhat comfortable	15(11)
		Neither	5 (6)	Neither	1 (4)
		Somewhat uncomfortable	3 (4)	Somewhat uncomfortable	2 (4)
		Very uncomfortable	0 (1)	Very uncomfortable	0 (4)
		Face recognition		Voice recognition	
		Very comfortable	6 (5)	Very comfortable	5 (4)
		Somewhat comfortable	10 (7)	Somewhat comfortable	10 (8)
		Neither	9 (10)	Neither	9 (9)
		Somewhat uncomfortable	4 (4)	Somewhat uncomfortable	4 (5)
		Very uncomfortable	1 (4)	Very uncomfortable	2 (4)
		Hand geometry		Signature	
		Very comfortable	6 (3)	Very comfortable	8 (5)
		Somewhat comfortable	12 (7)	Somewhat comfortable	13 (11)
		Neither	8 (11)	Neither	4 (3)
		Somewhat uncomfortable	3 (5)	Somewhat uncomfortable	4 (7)
		Very uncomfortable	1 (4)	Very uncomfortable	1 (4)
14	How acceptable do you feel it is to demand registration of biometric information for authentication in a	Eye (iris/retina)		Fingerprint	
		Very acceptable	9 (13)	Very acceptable	16 (11)
		Somewhat acceptable	15 (5)	Somewhat acceptable	11 (7)
		Neither	3 (6)	Neither	2 (3)

	system?	Somewhat acceptable 3 (5) / Very acceptable 0 (1); Somewhat acceptable 1 (6) / Very acceptable 0 (3) Face recognition: Very acceptable 7 (6) / Somewhat acceptable 12 (4) / Neither 5 (12) / Somewhat acceptable 6 (5) / Very acceptable 0 (3) Voice recognition: Very acceptable 7 (5) / Somewhat acceptable 11 (6) / Neither 5 (11) / Somewhat acceptable 7 (5) / Very acceptable 0 (3) Hand geometry: Very acceptable 10 (4) / Somewhat acceptable 9 (6) / Neither 4 (10) / Somewhat acceptable 7 (7) / Very acceptable 0 (3) Signature: Very acceptable 11 (8) / Somewhat acceptable 8 (7) / Neither 5 (5) / Somewhat acceptable 6 (6) / Very acceptable 0 (4)
15	How would you range biometric authentication vs. traditional authentication when it comes to user-friendliness?	Better 27 (23) / Worse 0 (2) / No difference 3 (5)
16	How would you range biometric authentication vs. traditional authentication when it comes to security?	Better 30 (17 / Worse 0 (3) / No difference 0 (10)
17	Which of these techniques do you feel is a secure form for authentication? That means that no one	Eye (iris/retina): Very secure 18 (16) / Somewhat secure 5 (9) / Neither 7 (4) Fingerprint: Very secure 19 (4) / Somewhat secure 9 (12) / Neither 0 (1)

<table>
<tr><td></td><td>can steal it from you, pretend that they are you, or you can lend it out to anyone?</td><td>
<table>
<tr><td>Somewhat insecure</td><td>0 (0)</td></tr>
<tr><td>Very insecure</td><td>0 (1)</td></tr>
</table>
</td><td>
<table>
<tr><td>Somewhat insecure</td><td>2 (9)</td></tr>
<tr><td>Very insecure</td><td>0 (4)</td></tr>
</table>
</td><td></td></tr>
<tr><td></td><td></td><td>Face recognition
<table>
<tr><td>Very secure</td><td>7 (2)</td></tr>
<tr><td>Somewhat secure</td><td>11 (13)</td></tr>
<tr><td>Neither</td><td>4 (7)</td></tr>
<tr><td>Somewhat insecure</td><td>7 (6)</td></tr>
<tr><td>Very insecure</td><td>1 (2)</td></tr>
</table>
</td><td>Voice recognition
<table>
<tr><td>Very secure</td><td>6 (2)</td></tr>
<tr><td>Somewhat secure</td><td>9 (6)</td></tr>
<tr><td>Neither</td><td>6 (13)</td></tr>
<tr><td>Somewhat insecure</td><td>8 (6)</td></tr>
<tr><td>Very insecure</td><td>1 (3)</td></tr>
</table>
</td><td></td></tr>
<tr><td></td><td></td><td>Hand geometry
<table>
<tr><td>Very secure</td><td>8 (2)</td></tr>
<tr><td>Somewhat secure</td><td>14 (8)</td></tr>
<tr><td>Neither</td><td>4 (11)</td></tr>
<tr><td>Somewhat insecure</td><td>4 (5)</td></tr>
<tr><td>Very insecure</td><td>0 (4)</td></tr>
</table>
</td><td>Signature
<table>
<tr><td>Very secure</td><td>2 (0)</td></tr>
<tr><td>Somewhat secure</td><td>7 (6)</td></tr>
<tr><td>Neither</td><td>10 (10)</td></tr>
<tr><td>Somewhat insecure</td><td>8 (11)</td></tr>
<tr><td>Very insecure</td><td>3 (3)</td></tr>
</table>
</td><td></td></tr>
<tr><td></td><td></td><td>Password
<table>
<tr><td>Very secure</td><td>1 (1)</td></tr>
<tr><td>Somewhat secure</td><td>8 (12)</td></tr>
<tr><td>Neither</td><td>8 (7)</td></tr>
<tr><td>Somewhat insecure</td><td>10 (9)</td></tr>
<tr><td>Very insecure</td><td>3 (1)</td></tr>
</table>
</td><td>ID-card
<table>
<tr><td>Very secure</td><td>1 (0)</td></tr>
<tr><td>Somewhat secure</td><td>9 (12)</td></tr>
<tr><td>Neither</td><td>7 (7)</td></tr>
<tr><td>Somewhat insecure</td><td>11 (9)</td></tr>
<tr><td>Very insecure</td><td>2 (2)</td></tr>
</table>
</td><td></td></tr>
<tr><td>18</td><td>If you were to decide, which technique would you prefer, and why?</td><td colspan="3">See Appendix D</td><td></td></tr>
</table>

Table 4: Presentation of the results from the survey.

6 Analysis and discussion of results

Chapter 1.4 proposed the following hypotheses:

- H1: End-users will quickly accept biometric authentication systems ($\mu<3.0$).
- H2: After a demonstration on how a biometric authentication system can be fooled, end-users will change their opinion of such an authentication system to a lower level of trust ($\mu \geq 0.0$).
- H3: End-users are not aware of, or have knowledge about privacy and technology issues to set requirements to registration, storage, and management of their biometric information.

To test H1 and H2, an expectation variable,μ was used. The value of μ can in reality be any given value in the range (1) to (5) (from the questionnaires). Why 3.0 is chosen for H1, and 0.0 is chosen for H2 will be explained in Chapter 6.1 and 6.2 respectively.

Factors that might influence the answers are the demographic data in part 1 of the questionnaire. Another thing that would be interesting to see, was if there was a difference between the participants of whom the false finger worked, and the participants of whom the false finger did not work. Unfortunately the author had too little time to investigate if there were any significant differences between the groups, but the results indicate that the differences are insignificant. During the time of the study, other ideas came up that would have improved the study, or answered other interesting questions. These ideas have been presented in Chapter 8.

6.1 Analysis H1

To answer the first hypothesis, only the answers from the first questionnaire were used. Before answering these questions, the participants were shown a demonstration of how a fingerprint authentication device recognizes a persons' fingerprint, see Chapter 4 on how the demonstration was carried out.

An earlier study [Helk], carried out at Sykehuset Innlandet together with Gjøvik University College explores issues when it comes to user authentication. It is therefore assumed before this study that users have one or more authentication issues they are concerned about. The situation at the hospital today is that many of the users are required to remember several usernames and/or passwords and these have to be changed from time to time. There is no guarantee that these passwords are required to be changed at the same time, which complicates the situation for the users even more. A single-sign-on system would have simplified the situation when it comes to user

convenience, but this is not a secure solution since the users might know each others passwords. The hospital has considered biometric authentication as a supplement or replacement for the traditional authentication systems.

According to the answers from the first questionnaire, 24 of the participants had heard of biometric authentication before the experiment. The remaining 6 had not. This observation might be good for the experiment because then the participants had some idea of what is asked about in the questionnaire and talked about in the experiment. For those who did not know much about biometric authentication, some information was provided in the questionnaire. Only 2 of the participants had provided their biometric information for authentication use in another situation, which also must be seen as good for this experiment since the demonstration was the first experience with biometric authentication for most of the participants.

In Question 13 the participants were asked to range how comfortable they were regarding the registering and usage of their biometric authentication. The level of comfort ranges from 'Very comfortable' (1) to 'Very uncomfortable' (5) for six biometric techniques. Generating a histogram of each variable shows that most of the participants have rated most of the variables from (3) to (1). Figures 15a and 15b shows the histograms for the level of comfort of eye biometrics and fingerprints. A close to similar distribution was observed for the variables from Question 14 to 17 as well.

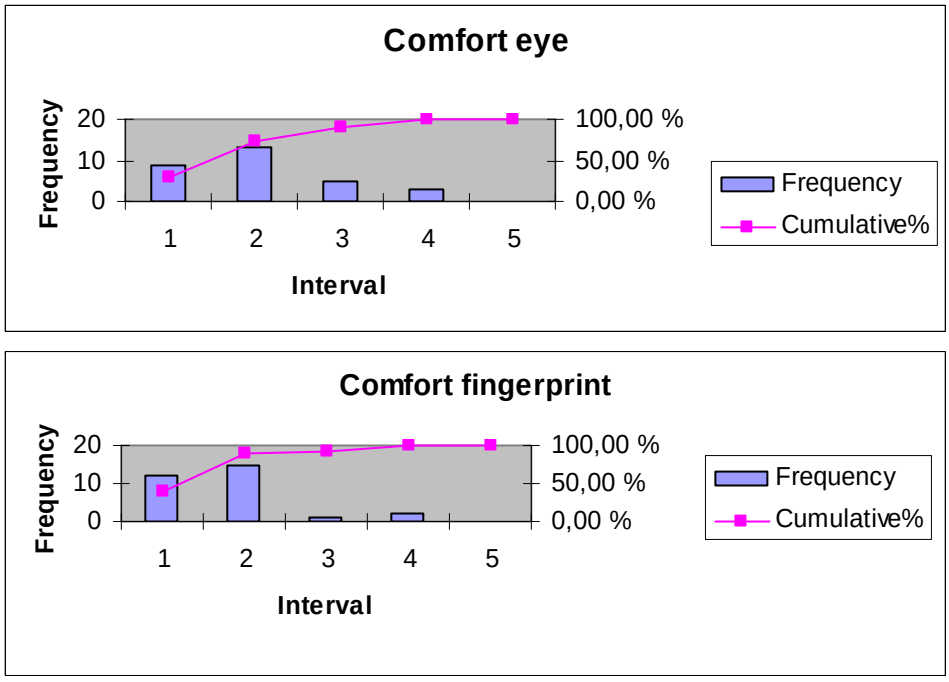


Figure 15 a and b: Histograms for the level of comfort of eye biometrics and fingerprints from the

first questionnaire.

The hypothesis can accordingly be written with the following 0-hypothesis (μ is the expected value):

H01: End-users will not so easily accept biometric authentication systems ($\mu \geq 3.0$).

H11: End-users will quickly accept biometric authentication systems ($\mu < 3.0$).

This means that if a participant has answered (1) or (2) he or she is assumed to quickly accept biometric authentication. If the participant answers (3) or higher, he or she is assumed not to accept biometric authentication so quickly.

To answer the hypotheses it is possible to use the student-t distribution. This distribution calculates the different confidence intervals of the sets of data, and says something about what can be expected if the questionnaire is performed a second time. Both the 95% and the 99% confidence intervals have been found using the following formulas [Løvå]:

$$\left[\overline{x} - t_{\alpha/2}^{(n-1)} \cdot \frac{S}{\sqrt{n}}, \overline{x} + t_{\alpha/2}^{(n-1)} \cdot \frac{S}{\sqrt{n}} \right]$$

$\overline{x}$ is the average of the values in the dataset, $t_{\alpha/2}$ is the quintile which is dependent on $^{(n-1)}$, the level of freedom. The t-value can be found in a table in most statistic books. S is an estimate of the standard deviation, and n is the number of observations, in this case 30. The calculated confidence intervals can be found in Tables 5, 6 and 7, together with summarizations for the level of comfort, level of acceptability, and level of security. The variables in the tables have been ranged from the summarizations of the level they have achieved. In the questionnaires it was possible to range a variable from (1), to (5) where (1) is the highest level and (5) is the lowest.

Biometric technique	Level of comfort summarized	Avg.	Standard deviation	95% confidence interval		99% confidence interval	
				Lower limit	Upper limit	Lower limit	Upper limit
Fingerprint	53	1,767	0,817	1,462	2,072	1,355	2,178
Eye biometrics	62	2,067	0,944	1,714	2,419	1,591	2,542
Signature	67	2,233	1,104	1,821	2,646	1,678	2,789

Hand geometry	71	2,367	1,033	1,981	2,752	1,847	2,887
Face recognition	74	2,467	1,074	2,066	2,868	1,926	3,007
Voice recognition	78	2,600	1,133	2,177	3,023	2,030	3,170

Table 5: Level of comfort summarized for question 13, questionnaire 1.

The lower the value in column 2, the higher level of comfort is registered. Remember that 'Very comfortable' takes the value (1), and 'Very uncomfortable' takes the value (5). It is clear to see that fingerprints has the highest level of comfort in this study, however a factor that might have had an effect on this result is the demonstration of the fingerprint authentication system before the questionnaire. If a similar study is to be performed later, it would be interesting to let the participants complete a questionnaire before the demonstration as well, to see if there is a difference from these results, see Chapter 13.

The same summarization can be done with level of acceptability and level of security, hence the following tables can be made, Table 6 and 7:

Biometric technique	Level of acceptability summarized	Avg.	Standard deviation	95% confidence interval		99% confidence interval	
				Lower limit	Upper limit	Lower limit	Upper limit
Fingerprint	48	1,600	0,770	1,312	1,888	1,212	1,988
Eye biometrics	60	2,000	0,910	1,660	2,340	1,542	2,458
Signature	66	2,200	1,157	1,768	2,632	1,618	2,782
Hand geometry	68	2,267	1,172	1,829	2,704	1,677	2,857
Face recognition	70	2,333	1,061	1,937	2,730	1,799	2,867
Voice recognition	72	2,400	1,102	1,989	2,811	1,846	2,954

Table 6: Level of acceptability summarized for question 14, questionnaire 1.

The techniques results in the same order in level of acceptability as with level of comfort. It is also here important to understand that the fingerprint authentication demonstration might have an effect on the results.

Technique	Level of security summarized	Avg.	Standard deviation	95% confidence interval		99% confidence	
				Lower limit	Upper limit	Lower limit	Upper limit
Fingerprint	45	1,500	0,820	1,194	1,806	1,087	1,913
Eye biometrics	49	1,633	0,850	1,316	1,951	1,205	2,061
Hand geometry	64	2,133	0,973	1,770	2,497	1,644	2,623
Face recognition	74	2,467	1,196	2,020	2,913	1,865	2,913
Voice recognition	79	2,633	1,189	2,190	3,077	2,035	3,231
Signature	93	3,100	1,094	2,692	3,508	2,550	3,650
ID-card	94	3,133	1,064	2,744	3,522	2,609	3,657
Password	96	3,200	1,042	2,803	3,597	2,665	3,735

Table 7: Level of security summarized for question 17, questionnaire 1.

When the participants rated their believed level of security, the results were similar to the results in level of acceptability and level of comfort. The exception was with the signature, which was rated three levels lower for security. For the security question, the participants could also rate ID-card and password. These two ended up as the last two techniques for security in an authentication system.

The confidence intervals says something about what can be expected if the survey is performed a second time. For example if a 30 new participants are asked the same questions, it is 95% likely that their average answers on the question level of security for fingerprints is in the interval [1.194, 1.806], and 99% likely that their answers is in the interval [1.087, 1.913], which again means that most of the participants will either answer (1) or (2) on this question.

Indications why H11 holds and H01 have to be rejected:

- First, the calculations performed should be statistical proof enough. H11 says that if $\mu<3.0$, H01 must be rejected. Reading the tables above, both the 95%, and 99% confidence intervals for; Fingerprint, Eye biometrics, Hand geometry, and Face

recognition have upper limits lower than 3.0. Only Voice recognition and Signature have upper limits above 3.0, however not for some of the intervals. This means that H01 must be rejected for the first four, but kept for the last two.

- Second, the summarized levels of comfort, acceptability, and security have very low values especially for fingerprint and eye biometrics. This indicates that the participants find them between very and somewhat comfortable, acceptable, and secure.
- In addition, the answers to the following questions support the statistical results:
- In question 15, the participants were asked to rate biometric authentication versus traditional authentication when it comes to user-friendliness. 90% answered they thought that biometric authentication was more user-friendly, and 10% thought there were no difference.
- In question 16, the participants were asked to rate biometric authentication versus traditional authentication when it comes to security. A 100% answered they thought that biometric authentication was more secure.
- The answers provided in question 18, see Appendix E, indicate clearly that the participants quickly would accept a biometric authentication system. 96% answered that they would prefer fingerprint recognition, eye biometrics, or biometric authentication, while only 4% answered that they would prefer traditional passwords.
-

These quantitative and qualitative answers indicate that it should be reasonable to think that users quickly will accept a biometric authentication system.

An important observation is that if the demand is that a lower value (2.5) is going to be used as μ, the conclusion will be a bit different, because then the confidence intervals must be no higher than 2.5. In this case, H01 will only be rejected for Fingerprint and Eye biometrics. H2: End-users will change their opinion of biometric authentication systems after a demonstration on how a biometric authentication system can be fooled.

6.2 Analysis H2

To answer the second hypothesis, the answers from both the first and the second questionnaire was used. Before answering the questions in the second questionnaire the participants was shown a demonstration of how a fingerprint authentication device recognizes a persons' fingerprint as in 6.1, but also how the same fingerprint authentication device can be fooled in an easy way, see Chapter 4 on how the demonstration was carried out.

As in 6.1 histograms of the variables from questionnaire 2 shows how the variables in the questions 13 to 17 are distributed. Figure 16a and Figure 16b shows the histograms for the level of comfort of eye biometrics and fingerprints.

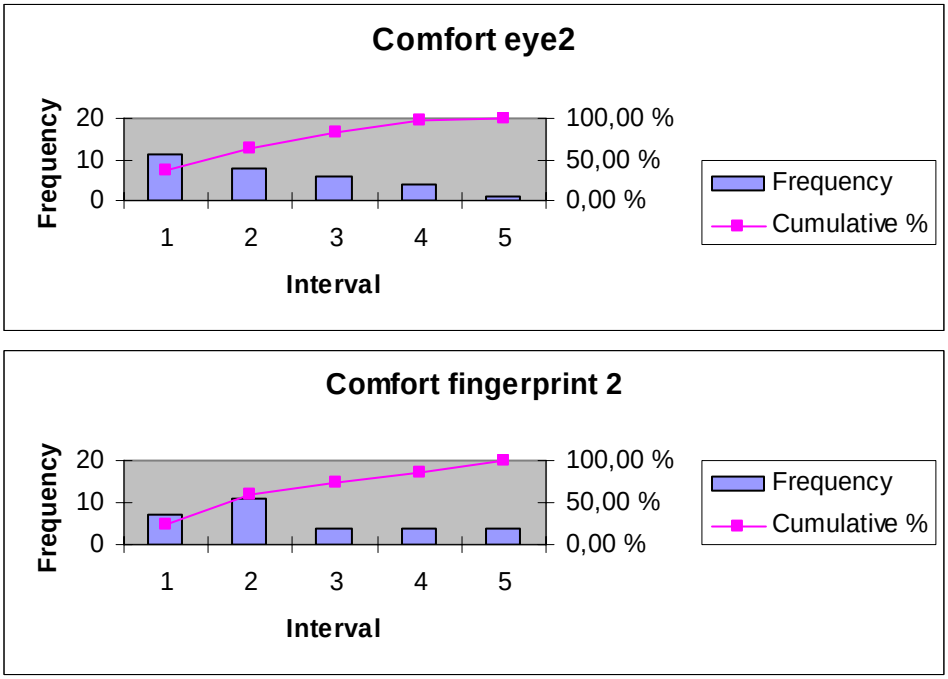


Figure 16 a and b: Histograms for the level of comfort of eye biometrics and fingerprints from the second questionnaire.

The hypothesis can be written with the according 0-hypothesis as follows:

H02: The opinion end-users have of biometric authentication systems will not change to a lower level after a demonstration on how a biometric authentication system can be fooled ($\mu \geq 0.0$).

H12: H2: After a demonstration on how a biometric authentication system can be fooled, end-users will change their opinion of such an authentication system to a lower level ($\mu < 0.0$).

This means that if the change in summarized level of comfort, acceptability, and security is 0 or higher, the participants have ranged the variable with a higher value, and hence a lower level. If a participant changes his or her opinion from (1) very comfortable to (4) uncomfortable, he or she has changed the opinion with a value of +3.

The different biometric techniques was ranged as in 6.1 and provided in Table 8.

Biometric technique	Level of comfort summarized	Change from Q1	Average	Standard deviation
Eye biometrics	66	+4	2,200	1,186
Fingerprint	77	+24	2,567	1,357
Signature	84	+17	2,800	1,349
Face recognition	85	+11	2,833	1,262
Voice recognition	87	+9	2,900	1,242
Hand geometry	90	+19	3,000	1,174

Table 8: Level of acceptability summarized for question 13, questionnaire 2.

It is interesting to see that all the biometric techniques have changed in a way that the participants found them more uncomfortable after the demonstration of the false fingerprint. Note that fingerprint is the variable that has changed the most, with hand geometry as the one changing second most.

The same summarization was also done with level of acceptability and level of security, hence the following tables were made, Table 9 and 10:

Biometric technique	Level of acceptability summarized	Change from Q1	Average	Standard deviation
Eye biometrics	66	+6	2,200	1,270
Fingerprint	73	+25	2,433	1,431
Signature	81	+15	2,700	1,418
Face recognition	85	+15	2,833	1,234
Voice recognition	85	+13	2,833	1,206
Hand geometry	89	+21	2,967	1,189

Table 9: Level of acceptability summarized for question 14, questionnaire 2.

The answers discover almost the same change here, with fingerprint and hand geometry changing the most.

Technique	Level of security	Change from	Average	Standard

	summarized	Q1		deviation
Eye biometrics	51	+2	1,700	0,952
Face recognition	83	+9	2,767	1,073
Password	87	-9	2,900	0,995
Fingerprint	87	+42	2,900	1,348
ID-card	91	-3	3,033	0,999
Hand geometry	91	+27	3,033	1,129
Voice recognition	92	+13	3,067	1,048
Signature	101	+8	3,367	0,928

Table 10: Level of security summarized for question 16, questionnaire 2.

This table probably provides the most interesting results. Here the participants also rate eye biometrics higher, or more secure, than fingerprints. But also face recognition and password have passed fingerprints in the participants' thoughts of level of security. Password and fingerprint gave the same values, but password was placed higher because it has decreased compared to Q1, while fingerprint has increased drastically (almost doubled). Also the value for hand geometry has increased compared to Q1. A reason of why the value of hand dynamics has increased in all three questions might have a combination of the increased fingerprint value; if the participants' rate fingerprints lower, they also might rate hand geometry lower, because fingers are a part of the hand (even if hand geometry authentication does not use fingerprints) the participant might think so.

The data in the last three tables are an indication to which variables are expected to reject H02, those with a + notation in the change from Q1 column. However, to analyze the data more correctly, they had to be normally distributed. By subtracting the results of Q2 from Q1 it is possible to achieve a normal distribution. Since the answer from the questionnaires might differ from (1) to (5) or (5) to (1), the interval for the normally distributed dataset is from -4 to +4. Figure 17 shows an example of the level of comfort for eye biometrics when the dataset is normally distributed. The rest of the normally distributed histograms can be found in Appendix D.

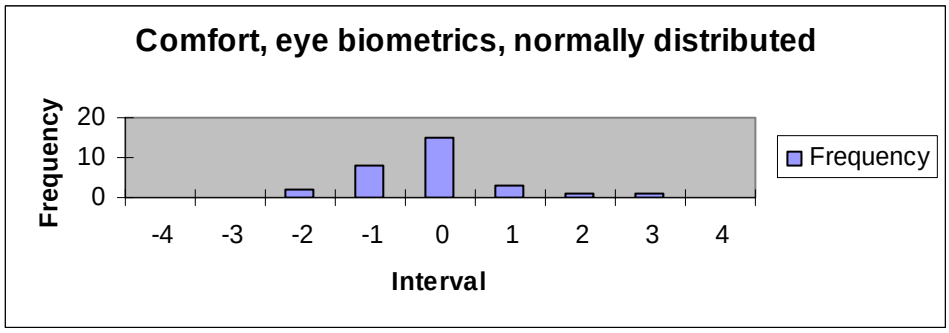


Figure 17: A histogram showing the differences between Q1 and Q2 when it comes to level of comfort on eye biometrics.

It is still possible to keep the same hypotheses, but now they will be tested against the confidence intervals made from the normally distributed datasets.

H02: The opinion end-users have of biometric authentication systems will not change to a lower level after a demonstration on how a biometric authentication system can be fooled ($\mu \geq 0.0$).

H12: H2: After a demonstration on how a biometric authentication system can be fooled, end-users will change their opinion of such an authentication system to a lower level ($\mu < 0.0$).

This means that if a variable, for example fingerprints has the upper confidence interval limit <0.0 for level of comfort, level of acceptability, and level of security, it can reject H02. The data has been tested against a 95% confidence interval and a 99% interval. The results from the normally distributed data will form the following Tables 11, 12, and 13 for level of comfort, level of acceptability, and level of security respectively:

Biometric technique	Level of comfort summarized	Average	Standard deviation	95% confidence interval		99% confidence interval	
				Lower limit	Upper limit	Lower limit	Upper limit
Eye biometrics	-4	-0,133	1,042	-0,522	0,542	-0,657	0,391
Fingerprint	-24	-0,800	0,997	-1,172	-0,428	-1,301	-0,299
Signature	-17	-0,567	1,104	-0,979	-0,154	-1,122	-0,011
Face	-11	-0,367	1,273	-0,842	0,108	-1,007	0,274
Voice	-9	-0,300	1,208	-0,751	0,151	-0,908	0,308
Hand	-19	-0,633	0,928	-0,980	-0,287	-1,100	-0,166

Table 11: Summarization and confidence intervals for level of comfort.

Biometric technique	Level of acceptability summarized	Avg.	Standard deviation	95% confidence interval		99% confidence interval	
				Lower limit	Upper limit	Lower limit	Upper limit
Eye biometrics	-6	-0,200	1,095	-0,609	0,209	-0,751	0,351
Face	-15	-0,500	1,253	-0,968	-0,032	-1,130	0,130
Fingerprint	-25	-0,833	1,261	-1,304	-0,362	-1,468	-0,198
Hand	-21	-0,700	1,119	-1,118	-0,282	-1,263	-0,137
Voice	-13	-0,433	1,278	-0,911	0,044	-1,076	0,210
Signature	-15	-0,500	1,480	-1,052	0,052	-1,245	0,245

Table 12: Summarization and confidence interval for level of acceptability.

Technique	Level of security summarized	Avg.	Standard deviation	95% confidence interval		99% confidence interval	
				Lower limit	Upper limit	Lower limit	Upper limit
Eye biometrics	-2	-0,067	0,868	-0,391	0,258	-0,504	0,370
Face recognition	-9	-0,300	1,119	-0,718	0,118	-0,863	0,263
Password	+9	0,300	1,236	-0,161	0,761	-0,322	0,922
Fingerprint	-42	-1,400	1,248	-1,866	-0,934	-2,028	-0,772
ID-card	+3	0,100	0,845	-0,215	0,415	-0,325	0,525
Hand geometry	-27	-0,900	1,125	-1,320	-0,480	-1,466	-0,334
Voice recognition	-13	-0,433	1,135	-0,857	-0,010	-1,004	0,138
Signature	-8	-0,267	1,172	-0,704	0,171	-0,857	0,323

Table 13: Summarization and confidence intervals for level of security.

As it is possible to read from the tables, at a 95% confidence interval, only fingerprint recognition and hand geometry have all three upper limits below 0. Hence it is only these two variables that can reject H02 at a 95% confidence interval. The participants' answers on the two variables have also changed to a lower enough level to reject the H02 hypothesis at a 99% confidence interval as well.

Several factors indicate that the end-users have changed their opinion:

- First, the calculations performed should give statistical proof. H12 says that if $\mu<0.0$, H02 must be rejected. Reading the tables above, both the 95%, and 99% confidence intervals for; Fingerprint and Hand geometry have upper limits lower than 0.0. Several of the other variables also have one or two out of three limits that are below 0.0, more on this in Chapter 12, conclusion. This means that H02 must be rejected for Fingerprint and Hand geometry, but kept for the last four.
- Second, the summarized levels of comfort, acceptability, and security, with exception for ID-card and password have increased in value. Especially for fingerprint and hand geometry which indicate that the demonstration have affected the participants.
- In question 15, the participants were asked to rate biometric authentication versus traditional authentication when it comes to user-friendliness. 76,67% answered they thought that biometric authentication was more user-friendly, 6,67% thought there were no difference, and 16,67% thought that traditional authentication was more user-friendly.

- In question 16, the participants were asked to rate biometric authentication versus traditional authentication when it comes to security. Only 56,67% (100% in questionnaire 1) thought biometric authentication was more secure, 10% though there were no difference, and 33,33% thought that traditional authentication was more secure.
-

These observations indicate that the demonstration has changed the way the participants look at biometric authentication.

6.3 Analysis H3

H03: End- users are aware, and have knowledge about privacy and technology to set the requirements to registration, storage, and management of their biometric information.

H13: End-users are not aware of, or have knowledge about privacy and technology issues to set requirements to registration, storage, and management of their biometric information.

This hypothesis is a bit more sophisticated and cannot easily be solved based on the quantitative date used to solve H1 and H2. However, the qualitative answers in question 18 gave some indications, see Appendix E:

- In the first questionnaire, 66% answered that they would choose fingerprint authentication if they were to choose system, 18% would choose eye biometrics, 2% would choose either eye or fingerprint, 9% would choose some sort of biometric authentication, and 4,5% would choose passwords.
-

Notice that this is after the demonstration of how the fingerprint sensor works when authenticating users. Most of the participants probably saw it as a great advantage compared to passwords, which they already have experienced can be used by a person it does not belong to, either authorized or unauthorized. This, together with the observation in H2, indicates that the participants easily would accept a biometric authentication system, without much attention to security aspects. The averages in Tables 5, 6, and7 in Chapter 6.1 tells the same, the participants mostly answered very- or somewhat comfortable, acceptable, and secure.

- In the second questionnaire, 32% answered that they would choose fingerprint authentication if they were to choose, 48% would choose eye biometrics, 4% didn't know, and 4% would choose ID-cards and passwords.

These numbers, together with the averages in Tables 8, 9, and 10 in Chapter 6.2, shows that the participants still would prefer biometric authentication even after a demonstration of fooling an authentication system. H2 shows that the participants have learned something since they rate the techniques lower in questionnaire 2 than in questionnaire 1, but since still about 1/3 choose fingerprint authentication in question 18, see Appendix E, this might indicate that the participants are not aware of, or have knowledge about how an unauthorized person can collect and use their biometric information.

6.4 Unforeseen events

Fingerprints from some of the participants matched the right fingerprint according to their profile, but also matched a fingerprint from another profile. In a biometric authentication system this would cause a false acceptance (see Chapter 2) because the system matched the wrong profile. Figure 18 shows an example where an artificial fingerprint matched two profiles, 'Finger ID 39' and Finger ID 42', in the database.

Some of the participants did not match their previously enrolled profile when trying to authenticate to the system. This is in an authentication system called false rejection, see Chapter 4, since the participant is enrolled and should be recognized by the system. This error can have two causes, the participant provided a bad fingerprint either when enrolling or when authenticating. Most likely it is not the enrollment that causes the error. This is because the system has a lower threshold value for how bad quality an enrolled fingerprint can have, and it also requires three good images for one enrollment. When the participant attempted to authenticate a second time the system recognized the provided fingerprint with the right profile, and the participant was accepted.

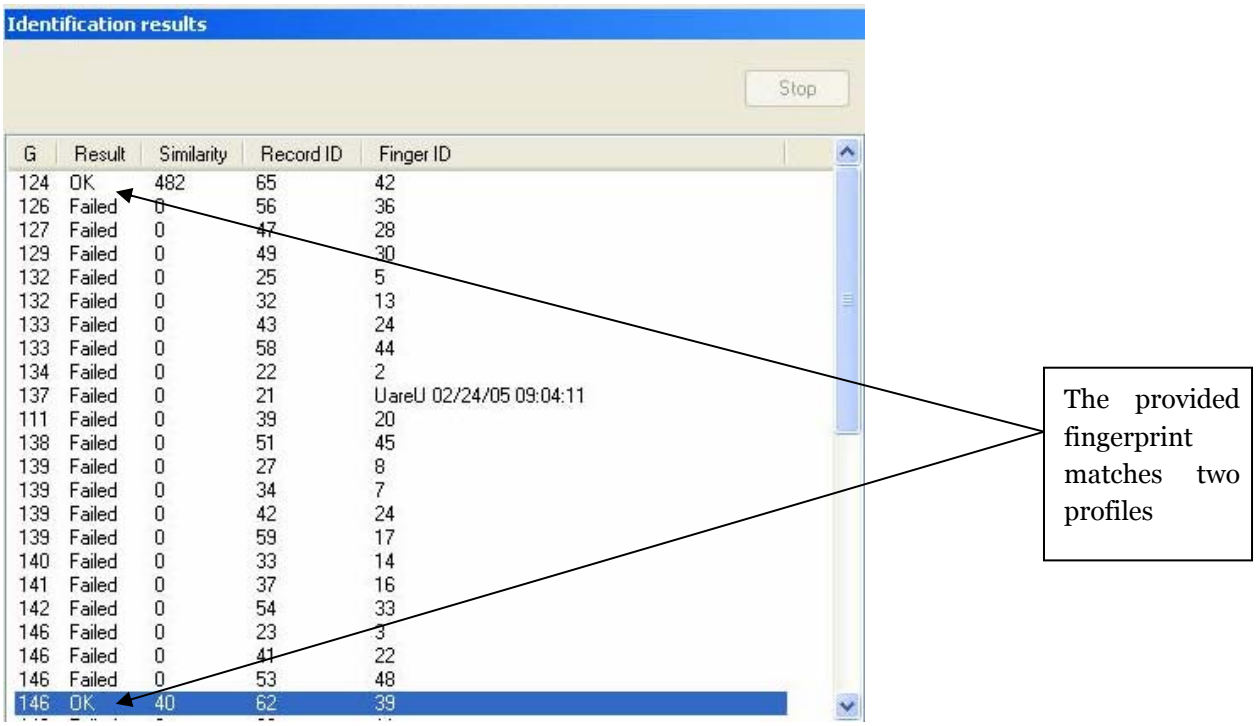


Figure 18: An attempt to authenticate matches two different profiles.

7 Conclusion

Research on and development of biometric authentication is increasing. Most agree that biometric authentication is the new era in automated authentication, and will replace or supplement traditional authentication. There are several publications that describe different approaches to authentication, but it is not possible to decide what the best authentication system is. Several factors have to be considered, most of them mentioned in Chapter 3.1, when choosing an authentication system.

The wide array of possibilities makes it difficult for both developers and implementers, but what about the end-users? A popular saying argues that 'Security is never stronger than the weakest link', and with the technology rapidly developing, users might find themselves as the weakest link. Adams and Sasse [Adam] once wrote an article, 'Users are not the enemy', based on a study that showed that users are not sufficiently informed and taught about security issues. They also argue that to develop a successful security system, the designers have to realize that they are the key. It is important for the users to know how the security systems should be used so that solutions that look good on paper will not fail in practice.

The results from this study show that end-users will most likely accept biometric authentication systems easily, probably without much concern for security. Several other studies have shown that most password users chooses a password that is very easy to obtain from an impostor, they write it down or just leave the computer unlocked. Adams and Sasse argue that authentication systems must be developed together with the end-users, because they are the ones who end up using the system, and the system is not secure if the users do not know how to use it correctly [Adam]. The results from this study say the same: Users should actively participate in the implementation of a biometric authentication system, not only be told what to do. By witnessing how such a system works, and what are the weaknesses of the system, the users develop an understanding of how to use the system in a better way.

This study also indicates that end-users should not been given most of the responsibility. The results from this study indicate that the end-users do not have enough knowledge or experience to use an authentication system the way it is supposed to. It is therefore necessary for a developer of an authentication system to observe how it is used, and evaluate threats.

A group of grocery stores in Germany have introduced fingerprint authentication as a way to pay for your groceries. The customers only have to press their finger against a

fingerprint sensor, and as long as there is money on the account they have made a payment. No password or ID-card is required. The only thing needed is your fingerprint. Both customers and employees are very satisfied. This is another example of the lack of knowledge. Wait and see when an impostor obtains a copy of someone's' fingerprint and starts buying groceries on someone else's account. If the users in Germany see that this system can be fooled, they probably would not use it. The results in this study support that statement.

Another research, 'Data Protection' performed by the European Commission in 2003 [Euro], looks at what view citizens of the European Union have about privacy and information security, and what level of trust they have of different businesses managing their private information. Especially the Nordic countries have a high rate of trust on different questions concerning privacy, which is somewhat similar to the results found in this study. In this study the average ratings on comfort ranged from 1.767 – 2.600, level of acceptability ranged from 1.600 – 2.400, and level of security ranged from 1.5 – 3.1 on a scale ranging from 1 to 5, where 1 is high level of trust. With 95% confidence intervals of 1.462 - 3.023, 1.312 – 2.811, and 1.194 – 3.508 respectively, this indicates that the participants have a high level of trust in authentication systems before they see with their own eyes that a biometric authentication system also can be fooled.

After seeing how easily an authentication system can be fooled, many of the participants changed their opinion about such systems. However, only for two of the techniques, fingerprint and hand geometry, the change was great enough to be seen as significant. Why the change of trust for the fingerprint technique was found significant is no surprise since this was the technique demonstrated. However, why the change of trust for the hand geometry technique was found significant is an interesting finding. The reason why this occurred might be because people think that hand geometry authentication makes use of the finger (prints). This finding should be explored further, and has been proposed in Chapter 8 – Recommendation for further work.

Some factors restrict the results in this study to be absolute. The participants may have provided the answers they did because of the place they work. Some might think it is not as necessary with high security at a hospital as for example in a bank. The study is also performed on a very small group of people. Several similar studies with larger and/or different groups should be done.

However, the results from this study give a clear indication on what to expect from a similar study at a later time, and they are also supported by previously research and publications.

8 Possible improvements and recommendations for further work

When working on this study, several ideas for improving the questions and the experiment, using different factors to improve or get more significant results have come to mind. Some of these are presented here:

- The questionnaires should be handed out to two different groups. The first group would be like the group in this experiment, while the second group also answers the questionnaires twice but without the demonstration on how a fingerprint authentication system works. This would make it possible to see if there is a difference between people who have seen the system in action and those who have not. Table 14 indicates the idea.

	1	2	3	4	5	6	7
Group A	Introduce the experiment	Demonstrate the fingerprint sensor	Copy fingerprint	Hand out Q1	Demonstrate how a sensor can be fooled	Hand out Q2	Analyze results
Group B	Introduce the experiment	-	-	Hand out Q1	-	Hand out Q2	Analyze results

Table 14: An alternative way to do the experiment.

- Another approach might be to do a similar study to this one, but in those cases where the artificial finger of the participant does not work, the participant shall not be shown that it is possible to fool the fingerprint sensor with a finger that you know works. The idea would be just like group A in Table 14, but at point 5 not every participant has the opportunity to see that a fingerprint authentication device can be fooled. This would make it possible to see if there is a difference between people who know that a fingerprint sensor can be fooled, and those who do not know. All participants would however know how the system works.
- A third approach might be to use different biometric authentication devices. It is believed that in this experiment, several of the participants were affected by the demonstration of the fingerprint authentication system, and hence it affected their answers regarding fingerprints. With a demonstration of different techniques and how they can be fooled, it is possible to find out if the results in this thesis are affected.
- Another way to find out if the results in this thesis are affected by the demonstration

might be to hand out three identical sets of questionnaires instead of two. Hand out the first questionnaire before any demonstration, and then do the experiment either like it has been performed here or like in the first suggestion.

- It is also possible to improve the quality of the artificial fingerprints, but then it will not be possible to see if there exists a difference between those where the false fingerprint worked and those where it did not work. By doing this the answers are based upon the same discovery from the participants, 'It is actually possible to make a perfectly usable artificial fingerprint from my own finger'. For more information on how to achieve better quality on the artificial fingerprints, see [Blom].
- Do one of the studies described above on two, or more, different groups of people. It can be interesting to see if there is a difference between for example skilled IT people versus people with lower IT skills.
- It would also be interesting to find out whether people believe fingerprints have something to do with hand-geometry recognition or not. Exploring this further will make it possible to say more about H3.

Bibliography

[Abbo] Abbott, J. Smart Cards: How Secure Are They? GSEC Practical v1.3, March 2002. Available online at: http://www.verifia.com/products/articles/2002-03-01.html

[Adam] Adams, A., Sasse, M., A. (1999). Users are not the enemy. In Communications of the ACM, Vol. 42, No. 12, December 1999.

[Basi] The Basic Card website; http://www.basiccard.com/

[Blom] Blommé, J. (2003). Evaluation of biometric security systems against artificial fingers. Master's thesis LITH-ISY-EX-3514-2003, Department of Electrical Engineering, Linköping University, Linköping, Sweden. Available online at: http://www.ep.liu.se/exjobb/isy/2003/3514/ [Accessed 15.02.2005].

[Boll] Bolle, R., Jain, A., Pankanti, S. (). Biometrics – Personal Identification in Networked Society. Kluwer Academic Publishers.

[Bros] Brostoff, S. and Sasse, M.A. (2000). Are Passfaces more usable than passwords: A field trial investigation. In People and Computers XIV - Usability or Else: Proceedings of HCI 2000 (Bath, U.K., Sept. 8-12, 2000). Springer Verlag, 405-424.

[BTT] Biometric Technology Today. Facial recognition proves to be no match for fingerprint technology. September 2004.

[Chel] R. Chellappa, S. Sirohey, C.I.Wilson, and C.S. Barnes, "Human and Machine Recognition of Faces: A Survey", University of MD, College Park, MD, 1994.

[Cole] Cole, S., A. Suspect Identities – A History of Fingerprinting and Criminal Identification. Harvard University Press, Cambridge, Massachusetts, London, England, 2001.

[Cran] Crane, H., D., Ostrem, J., S. "Automatic Signature Verification Using a Three-Axis Force-Sensitive Pen," IEEE Trans. on Systems, Man, and Cybernetics, Vol. SMC-13, No. 3, pp. 329-337, May-June 1983.

[Cres] Creswell, J., W. Research Design. Qualitative, Quantitative and Mixed Methods Approaches. Second Edition, SAGE Publications, 2003

[Digi] DigitalPersona webpage; http://www.digitalpersona.com/

[Euro] Special Eurobarometer 196, available at: http://www.datatilsynet.no/upload/Dokumenter/saker/2004/Hele%20undersøkelse.pdf

[FRVT] Phillips, P.J., Grother, P., Micheals, R.J, Blackburn, D.M., Tabassi, E., Bone, J.M. (2003) Face recognition vendor test 2002. Available online at: http://www.frvt.org/FRVT2002/documents.htm

[Garc] de Luis-Garcia, R., Lopez, C., A., Aghzout, O., Ruiz-Alzola, J. Biometric identification systems, Signal Processing. Volume 83, Issue 12, December 2003, Pages 2539-2557.

[Gorm] O'Gorman, L. Comparing Passwords, Tokens, and Biometrics for User Authetication. Proceedings of the IEEE, Vol. 91, No. 12, desember 2003.

[Harr] Harris, T. Howstuffworks: How fingerprint scanners work. Available at http://computer.howstuffworks.com/fingerprint-scanner2.htm

[Helk] Helkala, K. Interviews of health workers of Sykehuset Innlandet made by Kirsi Helkala in November 2004-January 2005.

[Henr] Henriksson, M. (2002). Analys av fingeravtryck. (Eng: Analysis of Fingerprints). Master's thesis LITH-ISY-EX-ET-0239-2002, Department of Electrical Engineering, Linköping University, Linköping, Sweden. Available online at: http://www.ep.liu.se/exjobb/isy/2002/239/ [Accessed 25.03.2005].

[INCI] InterNational Committee for Information Technology Standards (INCITS), 1st Working Draft – INCITS M1 Vocabulary Harmonization, 2003.

[Inma] Inman, K., Rudin, N. "An Introduction to Forensic DNA Analysis". CRC Press, Boca Raton, Florida, 1997.

[Jain] Jain, A. K., Prabhakar, S., Pankanti, S. Can Identical Twins be Discriminated Based on Fingerprints? Available online at: http://www.cse.msu.edu/cgi-user/web/tech/document?NUM=00-23

[Jain2] Jain, A. K., Ross, A., Prabhakar, S. An introduction to Biometric Recognition. Biometrics, Vol. 14, No. 1, January 2004.

[Kirb] Kirby, L. T. "DNA Fingerprinting, An Introduction", Oxford University Press, New York, 1992.

[Lee] Lee, H. C., Gaensslen, R. E. Advances in Fingerprint Technology. 2nd ed. Boca Raton, Florida, CRC Press, 2001.

[LiuS] Liu, S., Silverman, M. A Practical Guide to Biometric Recognition, IT Pro, January/February, Vol ??, No. ??, January 2003.

[Løvå] Løvås, G. 1999. Statistikk for universiteter og høgskoler. 3. opplag, Universitetsforlaget, 1999.

[Malt] Maltoni, D., Maio, D., Jain, A. K., Prabhakar, S. Handbook of Fingerprint Recognition. Springer, New York, 2003.

[Mans] Mansfield, T. Biometric authentication in the real world, Biometrics. Available online at:
http://www.npl.co.uk/scientific_software/research/biometrics/

[Mats] Matsumoto, T., Matsumoto, H., Yamada, K., Hoshino S. (2002). Impact of artificial "gummy" fingers on fingerprint systems. In proceedings of SPIE Vol. #4677, Optical Security and Counterfeit Deterrence Techniques IV, Yokohama, Japan, January 2002. Yokohama National University. Available online at: http://cryptome.org/gummy.htm

[Moen] Moenssens, A., A. Fingerprint techniques, Chilton Book Co., New York, 1971.

[Moor] Moore, G. The History of Fingerprints, February 2003. Available at http://onin.com/fp/fphistory.html

[Neur] Neurotechnologia website;
http://www.neurotechnologija.com/index.html

[NSD] Norsk Samfunnsvitenskaplig Datatjeneste's homepage. Available at: http://www.nsd.uib.no

[Obai] Obaidat, M., S., Sadoun, B. "Verification of Computer users using Keystroke Dynamics," IEEE Trans. on Systems, Man and Cybernetics, Vol. 27, No. 2, pp. 261-269,April 1997.

[Phil] Phillips, P., J., Martin, A., Przybocki, M., Wilson, C., L. An Introduction to Evaluating Biometric Systems, IEEE Computer, 56-63, February 2000.

[Plam] Plamondon R., Lorette, G. "Identity Verification from Automatic Processing of Signatures: Bibliography," in Computer Processing of Handwriting, R. Plamondon and C. G. Leedham, Eds., World Scientific Publishing Co., Singapore, pp. 65-85, 1990.

[Putt] van der Putte, T., Keunig, J. (2000). Biometrical Fingerprint Recognition: Don't get your fingers burned. In Proceedings of IFIP TC/8WG8.8 Fourth Working Conference on Smart Card Research and Advanced Applications, pages 289-303. Kluwer Academic Publishers, September 2000. Available online at: http://cryptome.org/fake-prints.htm

[Sand] Sandström, M. (2004). Liveness Detection in Fingerprint Recognition Systems. Master's thesis LITH-ISY-EX-3557-2004, Department of Electrical

Engineering, Linköping University, Linköping, Sweden. Available online at: http://www.ep.liu.se/exjobb/isy/2004/3557/ [Accessed 15.01.2005].

[Umph] Umphress, D., Williams, G. "Identity Verification Through keyboard Characteristics," International Journal Man-Machine Studies, Vol. 23, pp. 263-273, Academic Press, 1985.

[Waym] Wayman, J., L. Technical testing and evaluation of biometric identification devices. Biometrics: Personal identification in a Networked Society, Kluwer Academic Publishers, Dordrecht, 1999.

[Wood] Woodward Jr, J., D., Orlans, N., M., Higgins, P., T. Biometrics, McGraw-Hill/Osborne, California, 2003.

[Web1] The Free Dictionary – authentication. Available at http://www.thefreedictionary.com/authentication [Accessed at 19.01.2005]

[Web2] The Free Dictionary – biometric authentication. Available at http://www.thefreedictionary.com/biometric+authentication [Accessed 19.01.2005].

[Web3] Webopedia – Identification. Available at http://wi-fiplanet.webopedia.com/TERM/I/identification.html [Accessed 20.01.2005].

[Web4] Webopedia – Verification. Available at http://wi-fiplanet.webopedia.com/TERM/V/verification.html [Accessed 20.01.2005].

[Web5] Fingerprint cards. Available at http://www.fingerprint.se/biometrics_biometrics.asp [Accessed 12.02.2005].

[Web6] Webopedia – Authentication. Available at http://wi-fiplanet.webopedia.com/TERM/A/authentication.html [Accessed 20.01.2005].

[Web7] The Free Dictionary – Negative Identification. Available at http://www.thefreedictionary.com/negative%20identification [Accessed at 21.03.2005].

[Web8] The Biometric Group - How is 'Biometrics' Defined? Available at http://www.biometricgroup.com/reports/public/reports/biometric_definition.html [Accessed at 21.03.2005].

[Web9] The Biometric Group - How Do Identification and Verification Differ? Available at http://www.biometricgroup.com/reports/public/reports/identification_verification.html

[Web10] Webopedia – Identity. Available at http://wi-fiplanet.webopedia.com/TERM/I/identity.html

[Web11] Webopedia – Capture. Available at http://wi-fiplanet.webopedia.com/TERM/C/capture.html

[Web12] Webopedia – Enroll. Available at http://wi-fiplanet.webopedia.com/TERM/E/enrollment.html

[Web13] Webopedia – Reference template. Available at http://wi-fiplanet.webopedia.com/TERM/R/reference_template.html

[Web 14] Webopedia – Extraction. Available at http://wi-fiplanet.webopedia.com/TERM/E/extraction.html

[Web15] Webopedia – Matching. Available at http://wi-fiplanet.webopedia.com/TERM/M/matching.html

[Web16] Webopedia – False acceptance. Available at http://wi-fiplanet.webopedia.com/TERM/F/false_acceptance.html

[Web17] Webopedia – False rejection. Available at http://wi-fiplanet.webopedia.com/TERM/F/false_rejection.html

[Web18] Webopedia – Equal error rate. Available at http://wi-fiplanet.webopedia.com/term/e/equal_error_rate.html

[Web19] The Biometric Group - Which is the Best Biometric Technology? Available at http://www.biometricgroup.com/reports/public/reports/best_biometric.html

[Web20] The International Biometric Industry Association. Available at www.ibia.org

[Web21] The Nuclear Threat Initiative homepage. Available at http://www.nti.org/e_research/e6_glossary.html#d

[Web22] The biometric group - Is DNA a biometric? Available at http://www.biometricgroup.com/reports/public/reports/dna.html

[Web23] The Free Dictionary – fingerprint. Available at http://www.thefreedictionary.com/fingerprint

[Web24] The International Biometric Group. The Henry Classification System, 2003.

[Web25] The Biometric Group – Biometric types? Available at http://www.biometricgroup.com/reports/public/reports/biometric_types.html

Appendix

Appendix A1: Questionnaire (In Norwegian)

User's trust in Biometric Authentication Systems – Do not take the end-users for granted.

Spørreskjema

Denne undersøkelsen vil forsøke å kartlegge noe av brukernes holdninger ovenfor automatisk autentisering. Med autentisering menes hvordan du kan tilkjennegi at du er du når du for eksempel skal logge deg på et system eller komme deg inn i et område som er lukket for de som ikke har tilgang. Vennligst sett kryss i riktig rute.

1. Nummer:					
2. Kjønn:				Mann	Kvinne
3. Alder:	16 -20	20 - 30	30 - 40	40 - 50	50 +
4. Avdeling:				Radiografi	Laboratorium
5. Har du noen gang studert data/IT?			Ja	Nei	Vet ikke/ husker ikke
5a. Hvis ja, hvor lenge?:					

6. På hvilket nivå vil du si du er når det gjelder kunnskaper og bruk av data og IT?

Svært høyt	Høyt	Verken eller	Lavt	Svært lavt

7. Hvor ofte bruker du datamaskiner i arbeidet?

Flere ganger hver dag	En gang hver dag	1-3 ganger i uka	1-3 ganger i mnd	Sjeldnere/aldri

Når du logger på en datamaskin med et brukernavn og passord, utføres det en prosess i maskinen som går ut på å bekrefte at du er den du hevder du er. Dette kalles en autentiseringsprosess, hvor brukernavnet og passordet du taster inn sammenlignes med det som er det korrekte. Legg merke til at maskinen kun kan verifisere at rett brukernavn og passord har blitt tastet inn, den vet ingenting om hvem som har tastet dette. (Det kan for eksempel være noen som har gjettet seg til brukernavnet og passordet ditt).

Det finnes i dag tre ulike typer autentisering,

- noe du vet, dette kan for eksempel være et passord og er for tiden den vanligste måten for autentisering.
- noe du har, dette kan for eksempel være et kort med en magnetstripe eller ID-kort.
- noe du er, dette kan for eksempel være ditt fingeravtrykk, mønster i øyet eller stemmen din.

(Det kan også være en kombinasjon av disse, for eksempel et nøkkelkort kombinert med enPIN-kode).

8. Benytter du deg av autentisering når du logger på en datamaskin på jobb?

Ja	Nei	Vet ikke/Bruker ikke datamaskin på jobb

8a. Hvis ja, hva slags autentiseringsmekanisme (Id) bruker du? (se over).

Vet (passord eller lignende)	Har (Id kort eller lignende)	Er (Fingeravtrykk eller lignende)

9. Har du noen gang lånt utID-kortet eller fortalt passordet ditt til noen?

Ja	Nei	Husker ikke/Ønsker ikke svare

Nå vil du bli stilt noen spørsmål om biometrisk autentisering. Det er viktig at du svarer så oppriktig som mulig på disse. Sett kryss i riktig rute også her.
Biometrisk autentisering går i korte trekk ut på å bruke fysiske karakteristika eller personlig oppførsel som er unikt for hvert enkelt menneske. De mest vanlige biometriske verifiseringsteknikkene går ut på å se om for eksempel ditt fingeravtrykk, hånd, øye, ansikt eller stemme matcher det som tidligere ligger registrert om deg i systemet.
For eksempel hvis du bruker et fingeravtrykksystem vil du bli nødt til å plassere fingeren din på en fingeravtrykkleser når du logger inn i et system. Systemet vil så bruke fingeravtrykket du avgir og se om det stemmer overens med det som er registrert på deg fra tidligere. Hvis det stemmer vil du bli logget inn til systemet.
Biometrisk autentisering er på vei til å bli innført som en erstatning for tradisjonelle autentiseringsmetoder. For eksempel vil man kreve at innreisende til USA har biometriske opplysninger i passet.

10. Har du hørt om biometrisk autentisering før denne undersøkelsen?

Ja	Nei	Vet ikke

11. Har du noen gang gitt fra deg biometriske opplysninger om deg selv til bruk for autentisering i en eller annen situasjon?

Ja	Nei	Vet ikke

12. Har du noen gang benyttet en eller flere av disse biometriske teknikkene? (Hvis ingen, trenger du ikke svare)

Øye (Iris eller netthinne)	Fingeravtrykk	Ansikts-gjenkjenning	Stemme-gjenkjenning	Håndgeometri	Signatur

13. Hvor komfortabel er du med å registrere og bruke din biometriske informasjon? (Ett svar for hver teknikk.)

a) Øye (Iris eller netthinne)	Svært komfortabel	Ganske komfortabel	Verken eller	Lite komfortabel	Svært lite komfortabel
b) Fingeravtrykk	Svært komfortabel	Ganske komfortabel	Verken eller	Lite komfortabel	Svært lite komfortabel
c) Ansikts-gjenkjenning	Svært komfortabel	Ganske komfortabel	Verken eller	Lite komfortabel	Svært lite komfortabel
d) Stemme-gjenkjenning	Svært komfortabel	Ganske komfortabel	Verken eller	Lite komfortabel	Svært lite komfortabel
e) Håndgeometri	Svært komfortabel	Ganske komfortabel	Verken eller	Lite komfortabel	Svært lite komfortabel
f) Signatur	Svært komfortabel	Ganske komfortabel	Verken eller	Lite komfortabel	Svært lite komfortabel

14. Hvor akseptabelt synes du det er å kreve at man må registrere sine biometriske opplysninger for å få tilgang til et system og bli autentisert på denne måten ved hver innlogging? Dette vil da kunne være en erstatning til for eksempel passord eller id-kort. (Ett svar for hver teknikk)

a) Øye (Iris eller netthinne)	Svært akseptabel	Ganske akseptabel	Verken eller	Lite akseptabel	Svært lite akseptabel
b) Fingeravtrykk	Svært akseptabel	Ganske akseptabel	Verken eller	Lite akseptabel	Svært lite akseptabel
c) Ansikts-gjenkjenning	Svært akseptabel	Ganske akseptabel	Verken eller	Lite akseptabel	Svært lite akseptabel
d) Stemme-gje	Svært akseptab	Ganske akseptab	Verken eller	Lite akseptabe	Svært lite

nkjenning	el	el		l	aksepta bel
e) Håndgeom etri	Svært akseptab el	Ganske akseptab el	Verken eller	Lite akseptabe l	Svært lite aksepta bel
f) Signatur	Svært akseptab el	Ganske akseptab el	Verken eller	Lite akseptabe l	Svært lite aksepta bel

15. Hvordan vil du rangere biometrisk autentisering mot tradisjonell autentisering (passord) når det gjelder brukervennlighet?

Bedre enn tradisjon ell autentis ering	Dårligere enn tradisjon ell autentise ring	Ingen forskjell

16. Hvordan vil du rangere biometrisk autentisering mot tradisjonell autentisering når det gjelder sikkerhet?

Mer sikker enn tradisjon ell autentis ering	Mindre sikker enn tradisjon ell autentise ring	Ingen forskjell

17. Hvilke av disse teknikkene føler du er en sikker form for autentisering, det vil si at ingen stjele den av deg og utgi seg for å være deg eller at du kan låne den bort til noen? (Ett svar for hver teknikk)

a) Øye (Iris eller netthinne)	Svært sikker	Ganske sikker	Verken eller	Lite sikker	Svært lite sikker
b) Fingeravtry kk	Svært sikker	Ganske sikker	Verken eller	Lite sikker	Svært lite sikker
c) Ansikts-gje nkjenning	Svært sikker	Ganske sikker	Verken eller	Lite sikker	Svært lite sikker
d) Stemme-gje nkjenning	Svært sikker	Ganske sikker	Verken eller	Lite sikker	Svært lite sikker

e) Håndgeometri	Svært sikker	Ganske sikker	Verken eller	Lite sikker	Svært lite sikker
f) Signatur	Svært sikker	Ganske sikker	Verken eller	Lite sikker	Svært lite sikker
g) Passord	Svært sikker	Ganske sikker	Verken eller	Lite sikker	Svært lite sikker
h) Id-kort	Svært sikker	Ganske sikker	Verken eller	Lite sikker	Svært lite sikker

18. Hvis du skulle bestemme, hvilket system ville du foretrekke å bruke? Og hvorfor?

Takk for at du tok deg tid til å delta på denne undersøkelsen!

Appendix A2: Questionnaire (In English)

User's trust in Biometric Authentication Systems – Do not take the end-users for granted.

Questionnaire

This survey wishes to investigate some of the attitudes end-users have when it comes to automatic authentication. With authentication means how to verify who you are when for example logging onto a system or enter an area with restricted access. Pleas tick in the boxes that you feel matches you best.

1. Number:					
2. Sex:				Man	Woman
3. Age:	16 -20	20 - 30	30 - 40	40 - 50	50 +
4. Department:				Radiography	Laboratory
5. Have you ever studied computers/IT?			Yes	No	Don't know/Doesn't remember
5a. If yes, for how long?					

6. At what level do you feel you are when it comes to knowledge and usage of IT?

Very high	High	Neither	Low	Very low

7. How often do you use computers in daily work?

Several times a day	Once a day	1-3 times a week	1-3 times a month	Seldom/never

When you log on to a computer with a username and a password, a process which confirms who you are, is performed in the machine. This is called an authentication process. Where the username and password you enter is compared with the correct one stored in the database in the system. You should notice that the system only confirms that right username and password is entered. It does not know who entered this information. (For example if someone has guessed or found your username and password).

As of today three methods of authentication exists:

- Something you know, for example a password. This is the most used method of authentication today.
- Something you have, for example a card with a magnet stripe orID-card..
- Something you are, for example your fingerprint, eye, or your voice.

(These methods can also be combined, for example a keycard and aPIN-code).

8. Do you authenticate when logging onto a computer at work?

Yes	No	Don't know/Don't use computers at work

8a. If yes, what method of authentication do you use? (see above).

Know (password or similar)	Have (ID-card or similar)	Are (Fingerprint or similar)

9. Have you ever lend out yourID-card or told your password to anyone?

Yes	No	Don't remember/Don't want to answer

Now I will ask you some questions about biometric authentication. It is important that you answer as sincere as possible at these questions. (Also tick the right boxes).

Biometric authentication techniques use physical characteristics or personal behavior which is unique for every human being, to verify or identify people. The most common used biometric verification characteristics are fingerprint, hand geometry, eye biometrics, face recognition, and voice recognition.

Let us say you are using for example a fingerprint recognition system. Then you will be required to place your finger on a fingerprint sensor when logging on to the system. The system will take an 'image' of your fingerprint and verify this with one already in the system's database, which is provided by you earlier. If these fingerprints match you will be logged on to the system.

Biometric authentication is already on its way to replace, or complement traditional authentication methods. In the US it will soon be required with biometric information in traveler's passports.

10. Have you heard about biometric authentication before this experiment?

Yes	No	Don't know

11. Have you ever provided biometric information for use for authentication in any sort of situation?

Yes	No	Don't know

12. Have you ever used any of these biometric techniques to authenticate? (Don't answer if you have not used any)

Eye (Iris or retina)	Fingerprint	Face-recognition	Voice-recognition	Hand-geometry	Signature

13. How comfortable are you of registration and use of your biometric information? (One answer for each technique.)

a) Eye (Iris or retina)	Very comfortable	Somewhat comfortable	Neither	Somewhat un-comfortable	Very un-comfortable
b) Fingerprint	Very comfortable	Somewhat comfortable	Neither	Somewhat un-comfortable	Very un-comfortable

c) Face-recognition	Very comfortable	Somewhat comfortable	Neither	Somewhat un-comfortable	Very un-comfortable
d) Voice-recognition	Very comfortable	Somewhat comfortable	Neither	Somewhat un-comfortable	Very un-comfortable
e) Hand-geometry	Very comfortable	Somewhat comfortable	Neither	Somewhat un-comfortable	Very un-comfortable
f) Signature	Very comfortable	Somewhat comfortable	Neither	Somewhat un-comfortable	Very un-comfortable

14. How acceptable do you feel it is to demand registration of biometric information for authentication in a system? (One answer for each technique)

a) Eye (Iris or retina)	Very acceptable	Somewhat acceptable	Neither	Somewhat unacceptable	Very unacceptable
b) Fingerprint	Very acceptable	Somewhat acceptable	Neither	Somewhat unacceptable	Very unacceptable
c) Face-recognition	Very acceptable	Somewhat acceptable	Neither	Somewhat unacceptable	Very unacceptable
d) Voice-recognition	Very acceptable	Somewhat acceptable	Neither	Somewhat unacceptable	Very unacceptable
e) Hand-geometry	Very acceptable	Somewhat acceptable	Neither	Somewhat unacceptable	Very unacceptable
f) Signature	Very acceptable	Somewhat acceptable	Neither	Somewhat unacceptable	Very unacceptable

15. How would you range biometric authentication vs. traditional authentication when it comes to user-friendliness?

Better than traditional authentication	Worse than traditional authentication	No difference

16. How would you range biometric authentication vs. traditional authentication when it comes to security?

More secure than traditional authentication	Less secure than traditional authentication	No difference

17. Which of these techniques do you feel is a secure form for authentication? That means that no one can steal it from you, pretend that they are you, or you can lend it out to anyone? (One answer for each technique)

a) Eye (Iris or retina)	Very secure	Somewhat secure	Neither	Somewhat insecure	Very insecure
b) Fingerprint	Very secure	Somewhat secure	Neither	Somewhat insecure	Very insecure
c) Face-recognition	Very secure	Somewhat secure	Neither	Somewhat insecure	Very insecure
d) Voice-recognition	Very secure	Somewhat secure	Neither	Somewhat insecure	Very insecure
e) Hand-geometry	Very secure	Somewhat secure	Neither	Somewhat insecure	Very insecure
f) Signature	Very secure	Somewhat secure	Neither	Somewhat insecure	Very insecure
g) Password	Very secure	Somewhat secure	Neither	Somewhat insecure	Very insecure
h)ID-card	Very secure	Somewhat secure	Neither	Somewhat insecure	Very insecure

18. If you were to decide, which technique would you prefer, and why?

_____

Thank you for participating in this study!

Appendix B1: Information letter and Letter of Agreement (in Norwegian)

Forespørsel om å delta i spørreundersøkelse for Masteroppgaven: User's trust in Biometric Authentication Systems – Do not take the end-users for granted. Utført ved Høgskolen i Gjøvik og Sykehuset Innlandet.

Jeg er Masterstudent i Informasjonssikkerhet ved Høgskolen i Gjøvik og holder nå på med den avgjørende Masteroppgaven. Temaet jeg har valgt for oppgaven er Biometrisk autentisering, og jeg ønsker å undersøke hvordan mulige brukere forholder seg til tillit, holdninger og krav til slike systemer. For å undersøke dette ønsker jeg å utføre en kort undersøkelse på et utvalg av 40-50 personer som muligens vil kunne komme til å ta i bruk biometrisk autentisering enten i jobb eller privatliv. Jeg ønsker at du gjennomgår spørreundersøkelsen to ganger, tidspunkt for 2. gangs gjennomføring vil du få beskjed om via kontaktperson på sykehuset Gjøvik.

Spørsmålene vil forsøke å kartlegge noe av brukernes holdninger ovenfor automatisk autentisering. Med autentisering menes hvordan du kan tilkjennegi at du er du når du for eksempel skal logge deg på et system eller komme deg inn i et område som er lukket for de som ikke har tilgang. Med biometrisk autentisering menes å bruke fysiske karakteristika eller personlig oppførsel som er unikt for hvert enkelt menneske til å verifisere at du er den du er.

Slike verifiseringsteknikker kan for eksempel være ditt fingeravtrykk, avtrykk av hånd, skanning av øye, bilde av ansikt eller stemmegjenkjenning. I denne forbindelse vil du også bli bedt om å avlegge et fingeravtrykk. Av avtrykket du avgir vil det bli laget et kunstig fingeravtrykk til bruk ved 2. gangs gjennomføring av undersøkelsen. Jeg vil ikke komme til å bruke ditt kunstige fingeravtrykk uten at du selv er tilstede, og fingeravtrykket vil også holdes utilgjengelig for uvedkommende samt at du selv vil få muligheten til å ødelegge det når formålet er oppnådd.

Det er frivillig å være med og du har mulighet til å trekke deg når som helst underveis, uten å måtte begrunne dette nærmere. Dersom du trekker deg vil alle innsamlede data om deg bli slettet. Opplysningene vil bli behandlet konfidensielt, og ingen enkeltpersoner vil kunne kjenne seg igjen i den ferdige oppgaven. Opplysningene anonymiseres og opptakene slettes når oppgaven er ferdig, innen utgangen av 2005.

Dersom du ønsker å være med på undersøkelsen er det fint om du leser og skriver under på samtykkeerklæringen under og leverer den til meg sammen med spørreskjemaet.

Hvis det er noe du lurer på kan du ringe meg på xx xx xx xx, eller sende en e-post til henning@x.x.
Studien er meldt til Personvernombudet for forskning, Norsk samfunnsvitenskapelig datatjeneste A/S.

Med vennlig hilsen
Henning Gravnås

Samtykkeerklæring
for deltakelse i Masteroppgaven: User's trust in Biometric Authentication Systems – Do not take the end-users for granted ved Høgskolen i Gjøvik og Sykehuset Innlandet.

Jeg er informert om formålet med undersøkelsen. Jeg er også kjent med at opplysninger om meg blir behandlet strengt fortrolig og at undersøkelsen er meldt til Personvernombudet for forskning, Norsk samfunnsvitenskapelig datatjeneste AS, NSD.
Jeg er også kjent med at opplysningene vil bli behandlet konfidensielt, og ingen enkeltpersoner vil kunne kjenne seg igjen i den ferdige oppgaven.
Opplysningene anonymiseres og opptakene slettes når oppgaven er ferdig, innen utgangen av 2005.
Jeg samtykker i at svarene mine kan brukes til planlegging og forskning.
Jeg samtykker i at jeg på et senere tidspunkt kan bli kontaktet og få tilbud om å være med i nye undersøkelser.
Jeg samtykker i at det lages en kopi av min venstre tommels fingeravtrykk til bruk i denne undersøkelsen.
Jeg vet at jeg når som helst har mulighet til å trekke meg fra undersøkelsen uten å oppgi noen grunn, og at all informasjon jeg da har oppgitt vil bli slettet umiddelbart.

Du kan stryke det eller de punkter som du vil reservere deg mot.

Sted, dato	Underskrift

Appendix B2: Information letter and Letter of Agreement (in English)

Enquiry about participating in a survey for the Master thesis: User's trust in Biometric Authentication Systems – Do not take the end-users for granted, carried out at Gjøvik University College and Sykehuset Innlandet.

I am a Master student in Information security at Gjøvik University College. Now I am doing my final thesis work. The issue for the thesis is biometric authentication, and I want to find out what thoughts possible end-users have to such recognition systems. To investigate this I want to do a short study using the answers from 40-50 people who might become users of such a system within short time. I want you to go through the questionnaire twice, and time for the 2nd time will be given by a contact person at the hospital at Gjøvik.
The questions try to find out some of the users attitudes regarding automated authentication. Authentication means that you can verify that you are who you are when for example logging onto a system or gain access to a restricted area. Biometric authentication means to use physical characteristics unique to each human being to verify that you are who you claim to be. Such characteristics can for example be your fingerprint, hand dynamics, eye scan, face image or voice recognition. In this study you will be asked to make a fingerprint. An artificial fingerprint will be made out of this fingerprint and used at the 2nd time. Your fingerprint will not be used without you being present, and it will be kept away from strangers and you have the possibility to destroy the artificial fingerprint yourself when the demonstration as been performed.
It is voluntary to participate in this study and you can, at any time, withdraw from the study without giving a reason. If you decide to withdraw, all collected data from you will be deleted. The data will be handled confidentially, and no single persons will be able to recognize oneself in the finished thesis. The data will be anonymized, and deleted by the end of 2005.
If you decide to participate in this study I would like you to read and sign the letter of agreement and return it together with the questionnaire.
If you have any questions, I can be reached at number xx xx xx xx, or you can send an e-mail to henning@x.x.
The study has been reported to the Norwegian Social Science Data Services (in Norwegian: Norsk Samfunnsvitenskaplig Datatjeneste (NSD)).

Best regards
Henning Gravnås

Letter of Agreement
for participating in the Thesis: User's trust in Biometric Authentication Systems – Do not take the end-users for granted, carried out at Gjøvik University College and Sykehuset Innlandet, Hospital Gjøvik.

I have been informed of the purpose of this study. I also realize that information about me is handled confidential and that the study is reported to the Norwegian Social Science Data Services (in Norwegian: Norsk Samfunnsvitenskaplig Datatjeneste (NSD)).
I know that my information is handled confidential, and that no one can recognize oneself from the results in this study. The information will be anonymous, and any recordings and copies of fingerprints will be erased when the thesis work is done, 2005.
I consent that my answers can e used for planning and research.
I consent that I at a later stage can be contacted for participating in similar experiments.
I consent that a copy of the fingerprint of my left thumb is made for use in this experiment.
I have been informed that I can withdraw from the study at any time without reason, and that all information about me then will be erased at once.

You can cross out any points you want to reserve yourself against.

Place, date	Signature

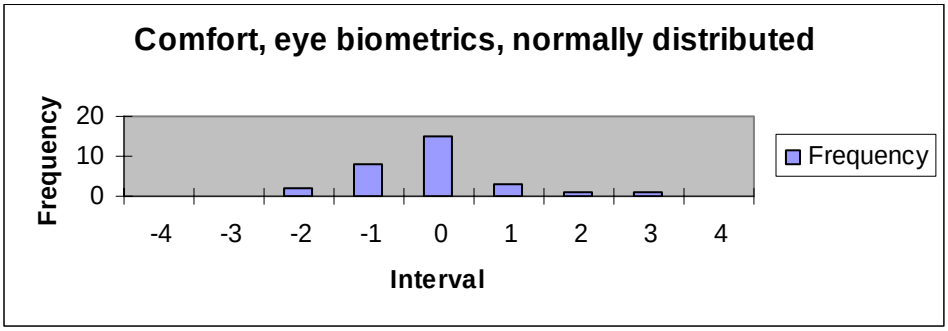
Appendix C: The History of Fingerprints

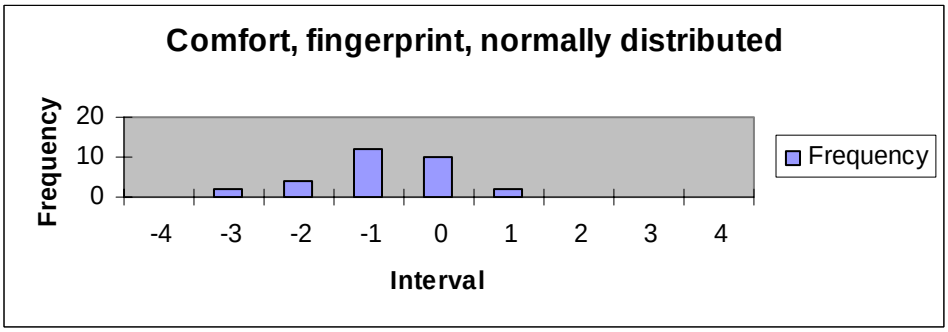
Time and place	Who	What was discovered	Additional sources
After 7000 BC in the Middle East, China and North America.	Native Americans, Palestinian, Assyrian and Chinese people.	Clay pottery or cave paintings sometimes contain fingerprint impressions probably placed to mark the identity of the potter or painter.	Lee and Gaensslen 2001, Moenssens 1971, Cole 2001.
1684, England.	The English plant morphologist Nehemiah Grew.	The first known published scientific paper reporting a systematic study on the ridge, furrow, and pore structure in fingerprints.	Lee and Gaensslen 2001.
1686, Italy.	The Italian Professor of Anatomy at the University of Bologna, Marcello Malpighi.	Described papillary ridges.	Cole 2001, Moore 2003.
1788.	Mayer.	Gave a detailed description of the anatomical formations of fingerprints, and identified a number of fingerprint ridge characteristics.	Moenssens 1971.
1809	Thomas Bewick.	Began to use his fingerprint as a trade mark. This is believed to be one of the most important milestones in scientific study of fingerprint recognition.	Moenssens 1971.
1823, Czech Republic.	The Czech Physician Jan Evangelista Purkyně.	Proposed the first fingerprint classification system. Purkyně classified fingerprints into nine categories according to the ridge configurations.	Moenssens 1971, Cole 2001.
1858, Bengal, India.	The Englishman William Herschel.	Started collecting prints from the whole hand or the right index and middle fingers to verify the identity when people signed contracts with the East-India Company.	Cole 2001.
1870s, Japan.	The Englishman Dr. Henry	Collected fingerprints from his students to determine if they changed over time. The first who used fingerprint	Beavin 2001, Faulds (in Nature) 1880,

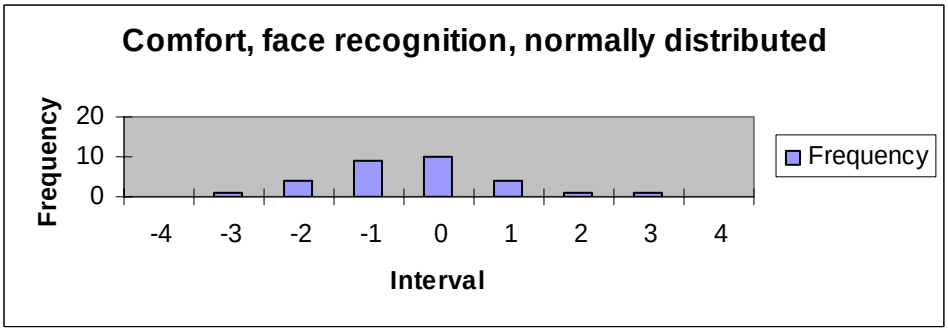
	Faulds.	recognition to help a criminal investigation. Faulds was also the first to suggest the individuality of fingerprints based on an empirical observation.	International Biometric Group – The Henry Classification System, 2003.
1888.	The British anthropologist, Sir Francis Galton.	Proved that fingerprints do not change over the lifetime of an individual, and that no two fingerprints are identical. Introduced the minutiae features, see Figure x.x, for fingerprint matching. Described the three classes; loop, arch, and whorl, later used by Sir Edward Henry.	Finger Prints by Francis Galton, 1892, Cole 2001, Moore 2003.
1892, Argentina.	The Argentine police officer Juan Vucetich.	Began the first fingerprint files based on Galton pattern types. Made the first criminal fingerprint taken to court.	
1899, India.	The Indian Azizul Haque for Sir Edward Henry.	The first robust system for classifying fingerprints was developed. Figure x.x. illustrates the differences between the three classes. The Henry System was used until the age of automated fingerprint recognition started in the 1960s - 1970s.	Classification and Uses of Finger Prints, Sir Edward Henry, Lee and Gaensslen 2001.
1901, Great Britain.	Scotland Yard.	Fingerprints were introduced for criminal identification. Other countries were soon to follow.	
1918.	Edmond Locard.	Proposed the “12 point rule” which suggested that if 12 points were the same between two fingerprints, it would suffice as a positive identification.	Moore 2003.
1924, U.S.A.	FBI	The FBI fingerprint identification division was set up with a database of 810.000 fingerprint cards.	Federal Bureau of Investigation (1984, 1991)
1960s	FBI, Home Office in the UK, and Paris Police Department.	The first computer processed fingerprint was introduced. Since then automated fingerprint identification systems (AFIS) have been deployed throughout the worlds law enforcement agencies.	Lee and Gaensslen 2001, M. Trauring “On the Automatic Comparison of Finger Ridge Patterns for Personal-Identity Verification.” Nature. 197, no. 4871 (1963): 938.
1980s		Fingerprint capture was made possible for non-criminal applications such as	[Wood]

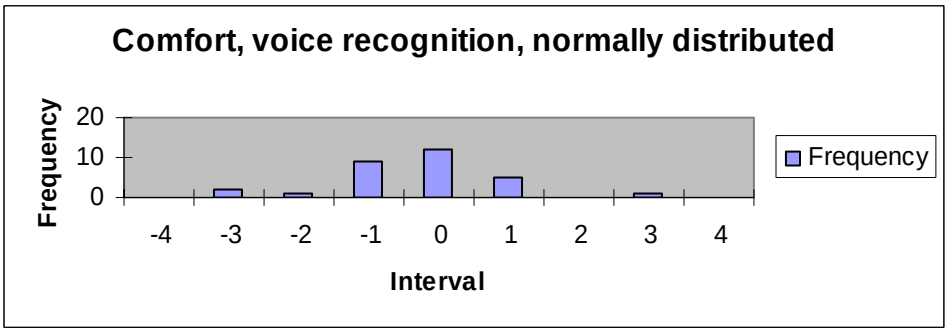
		ID-card programs. Leading research going on in Europe, USA, Canada, Japan, and Russia.	
1990s		Fingerprint authentication available on personal level, computers, mobile phones etc. Sagem Group purchased Morpho Systems and became the world leader in civil AFIS technology sales. Integrated Automated Fingerprint Identification System (IAFIS) is developed in the US.	J. Berry, "The history and development of fingerprinting," in Advances in Fingerprint Technology, (H. C. Lee and R. E. Gaensslen, ed.s), CRC Press, Florida, 1994, [Wood].
2004	FBI	FBI's IAFIS in Clarksburg, West Virginia, USA contains more than 46 million individual computerized fingerprints of known criminals.	

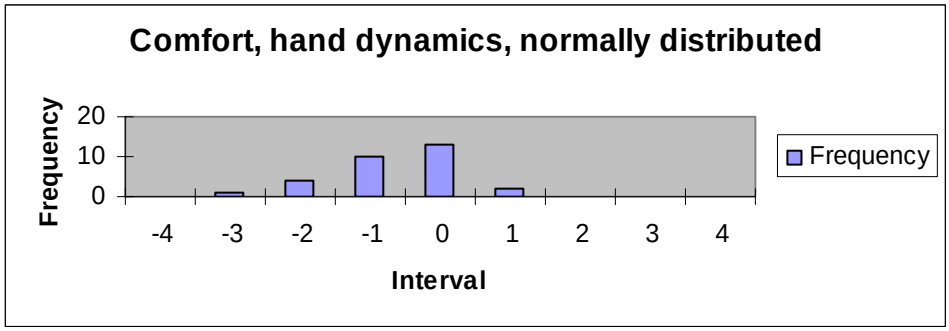
Appendix D: Normally distributed histograms from H2

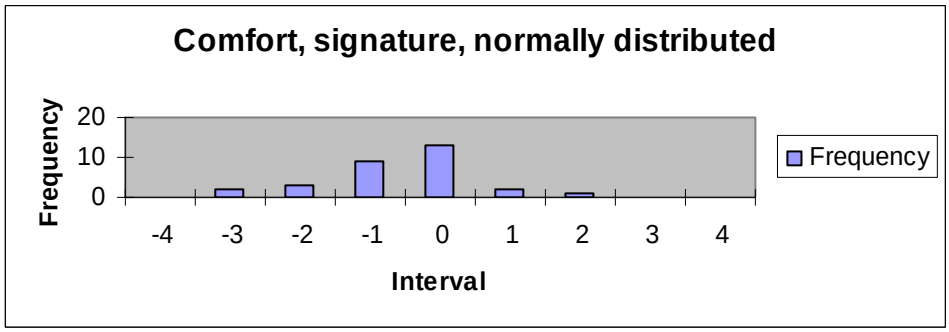


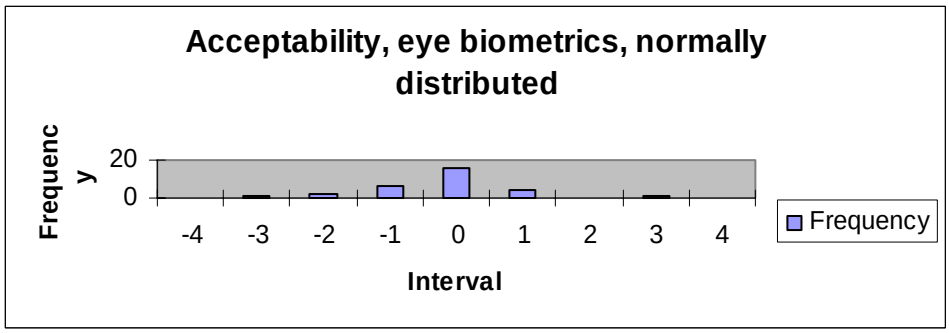


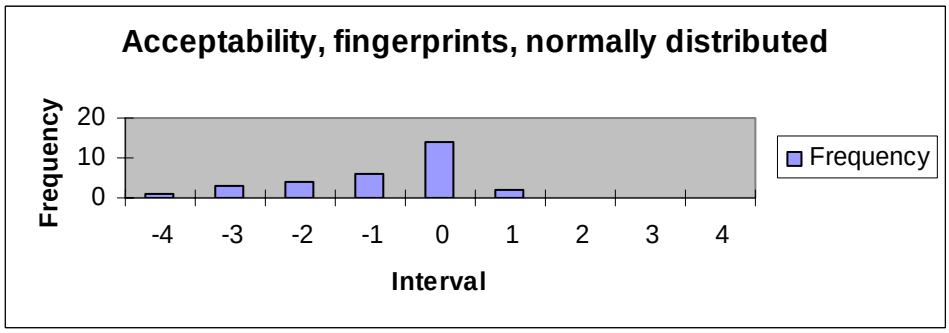


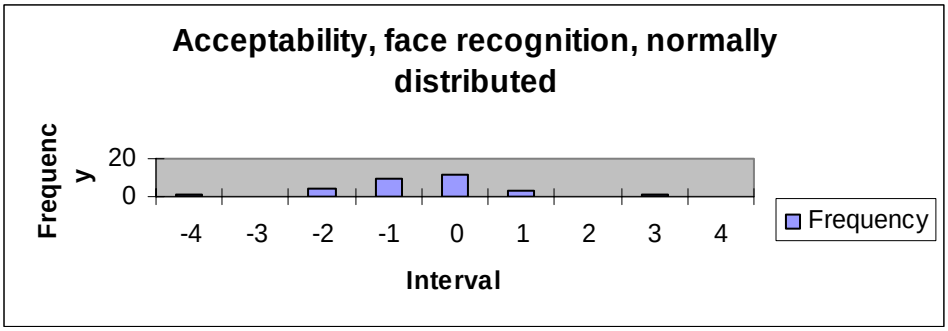


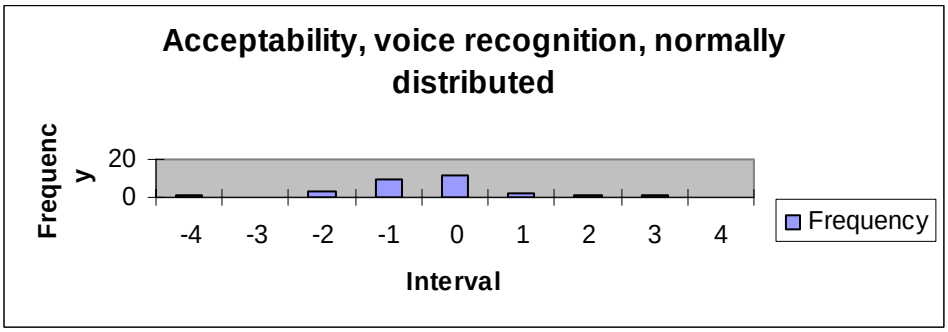

Comfort, hand dynamics, normally distributed
Frequency
20
10
0
-4 -3 -2 -1 0 1 2 3 4
Interval
Frequency

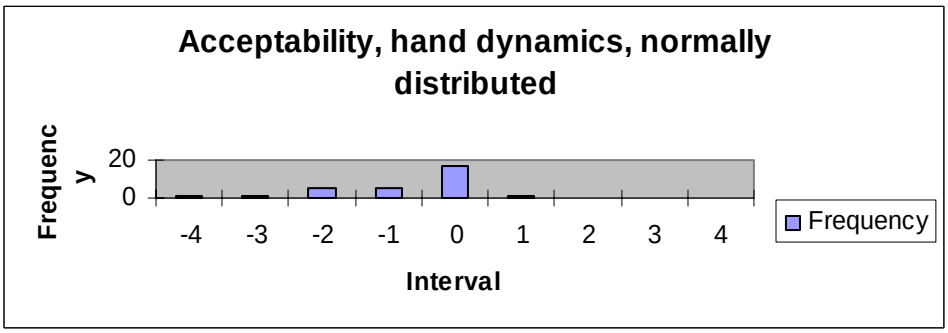

Comfort, signature, normally distributed
Frequency
20
10
0
-4 -3 -2 -1 0 1 2 3 4
Interval
Frequency

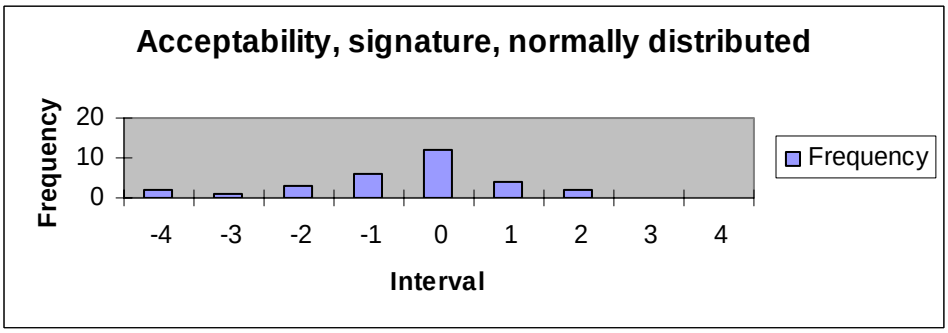

Acceptability, eye biometrics, normally distributed
Frequenc y
20
0
-4 -3 -2 -1 0 1 2 3 4
Interval
Frequency

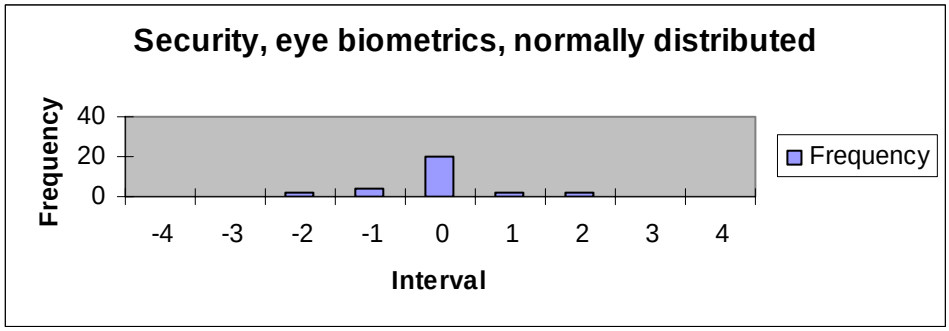

Acceptability, fingerprints, normally distributed
Frequency
20
10
0
-4 -3 -2 -1 0 1 2 3 4
Interval
Frequency

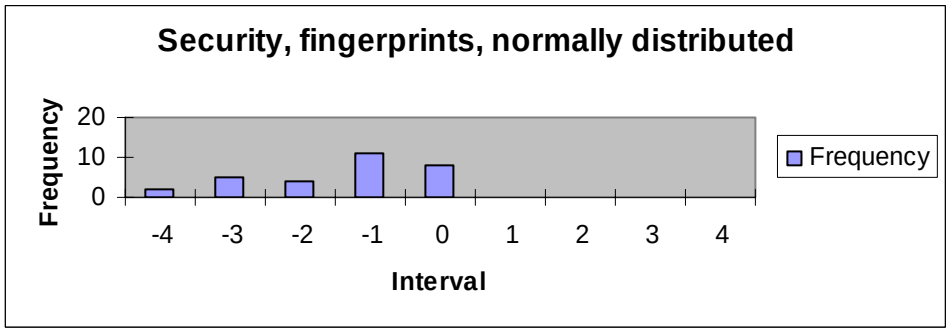

Acceptability, face recognition, normally distributed
Frequenc y
20
0
-4 -3 -2 -1 0 1 2 3 4
Interval
Frequency

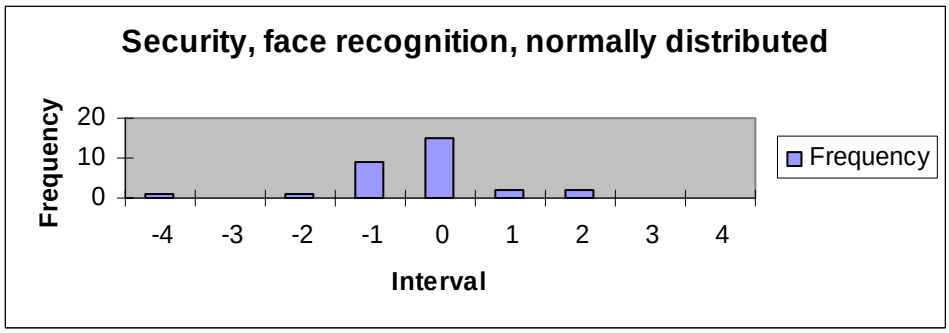

Acceptability, voice recognition, normally distributed
Frequenc y
20
0
-4 -3 -2 -1 0 1 2 3 4
Interval
Frequency

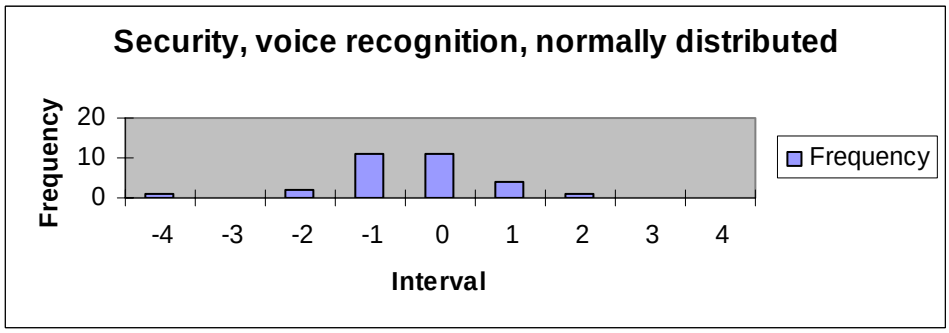

Acceptability, hand dynamics, normally distributed
Frequenc y
20
0
-4 -3 -2 -1 0 1 2 3 4
Interval
Frequency

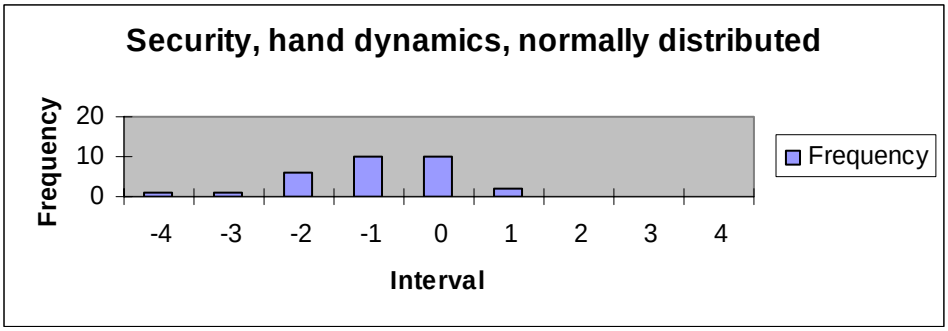

Acceptability, signature, normally distributed
Frequency
20
10
0
-4 -3 -2 -1 0 1 2 3 4
Interval
Frequency

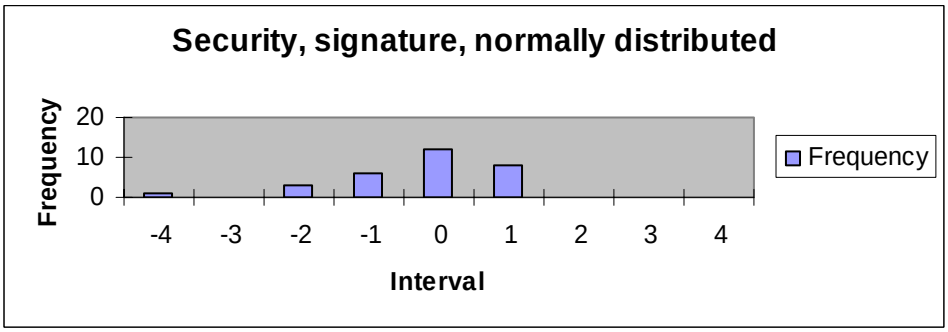

Security, eye biometrics, normally distributed
Frequency
40
20
0
-4 -3 -2 -1 0 1 2 3 4
Interval
Frequency

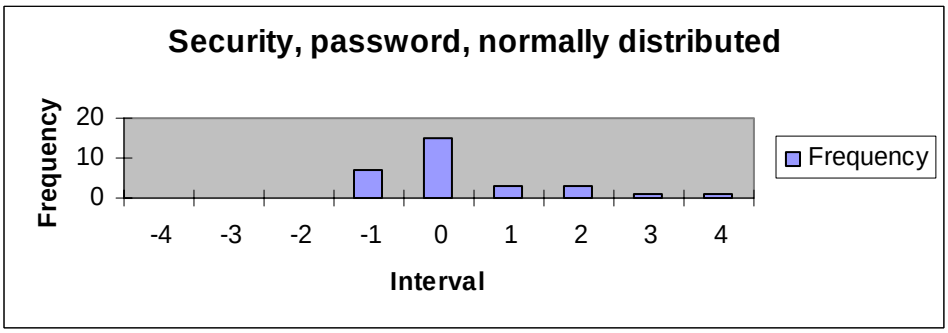

Security, fingerprints, normally distributed
Frequency
20
10
0
-4 -3 -2 -1 0 1 2 3 4
Interval
Frequency

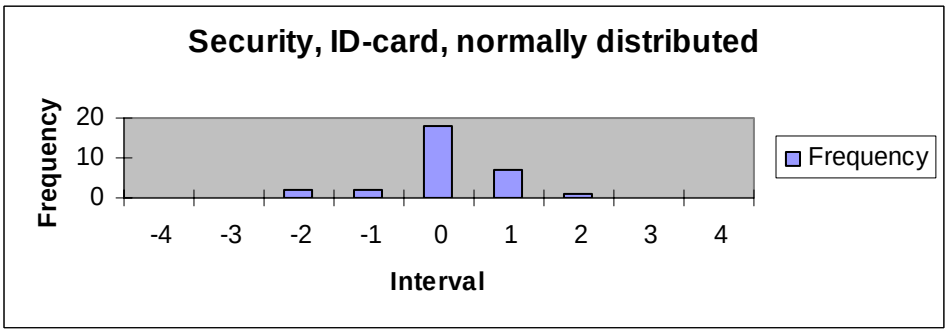

Security, face recognition, normally distributed
Frequency
20
10
0
-4 -3 -2 -1 0 1 2 3 4
Interval
Frequency


Security, voice recognition, normally distributed
Frequency
20
10
0
-4 -3 -2 -1 0 1 2 3 4
Interval
Frequency


Security, hand dynamics, normally distributed
Frequency
20
10
0
-4
-3
-2
-1
0
1
2
3
4
Interval
Frequency


Security, signature, normally distributed
Frequency
20
10
0
-4
-3
-2
-1
0
1
2
3
4
Interval
Frequency


Security, password, normally distributed
Frequency
20
10
0
-4
-3
-2
-1
0
1
2
3
4
Interval
Frequency


Security, ID-card, normally distributed
Frequency
20
10
0
-4
-3
-2
-1
0
1
2
3
4
Interval
Frequency

Appendix E: Answers from Question 18 (Norwegian)

This is a collection of the answers to Question 18.Only the summarization will be translated, see the end of the appendix.
I min jobb føler jeg at tommel/fingeravtrykk vil være en god løsning.
Fingeravtrykk
Høres veldig greit ut å bruke fingeravtrykk til å logge seg inn på PC og låse opp dører i stedet for å huske 3 forskjellige brukernavn og 5-6 forskjellige passord!
Ville nok velge det hvis det ble forsket nok til å lage et system som fungerer med minst mulig feilkilder!
Fingeravtrykk - Virker sikkert og enkelt i bruk
Fingeravtrykk, enkelt, slipper å huske passord. Sikkert
Fingeravtrykk, hvis lett å registrere -> Brukervennlig
Fingeravtrykk hvis det funker greit
Fingeravtrykk, enkelt å håndtere, sikkert.
Fingeravtrykk fordi det er sikkert og lettvint
Fingeravtrykk. Den er 100 % sikker, og alltid tilgjengelig
Fingeravtrykk. Unikt
Fingeravtrykk synes sikkert, og vi har jo 10 av dem, om vi skulle miste en finger i løpet av helgen. Tror færre vil prøve seg hvis sikkerheten ikke er så høy, pga prestisje
Fingeravtrykk
Fingeravtrykk; svært komfortabel og sikker.
Fingeravtrykk, sikkert og lettvint.
Fingeravtrykk! Virker enkelt og greit. Raskt, og umulig å kopiere.
Fingeravtrykk. Enkel og sikker metode.
Fingeravtrykk. Synes det er en sikker og grei måte å logge seg på
Fingeravtrykk virker fint. Slippe å huske passord.
Fingeravtrykk; mest sikker og unik for alle.
Fingeravtrykk. Enkelt å bruke og svært sikkert.
Fingeravtrykk: enkelt og lett tilgjengelig.
fingeravtrykk, virker mer praktisk
Fingeravtrykk. Helt spesielt for hver enkelt person.
Foretrekker fingeravtrykk. Enkelt i bruk. Unikt. Det er varig dersom jeg unngår fingerskader. Slipper å huske mange forskjellige passord.
Jeg vil foretrekke fingeravtrykk, en enkel og relativt sikker løsning. Imidlertid bør mer enn en finger være en del av identifiseringen (pga brannskade og lignende).
Biometrisk autentisering m/fingeravtrykk.
Har ikke tenkt så mye på det. Det virket veldig greit m/ fingeravtrykk. Hvor følsom er stemmegjenkjenning v/forkjølelse og lignende. Litt tvil om øye - hvordan en laser operasjon påvirker identiteten.
Jeg ville valgt systemet med biometrisk autentisering gjerne med fingeravtrykk, dersom systemet er optimalt/sikkert. Det ville gjøre det lettere for oss, da vi slipper å huske på mange passord.

Iris eller netthinne eller fingeravtrykk
Øye, meget sikker metode og vanskelig å stjele.
Øye (iris eller netthinne), fordi det virker som det er veldig sikkert.
Fingeravtrykk er også praktisk (lettvint).
Øye (iris eller netthinne) eller fingeravtrykk ville vært det mest praktiske og sikre. Man slipper da å huske alle passordene, og det er vanskeligere å misbruke.
Øye, el fingeravtrykk. Dette er en teknikk som ikke er lett å misbruke av andre personer, og av den grunn bedre personvern.
Øye- eller fingeravtrykk fordi det er unikt for hver bruker, og kan ikke brukes av andre.
Øye (iris eller netthinne) eller håndgeometri. Ser for meg at det er vanskelig å "kopiere" disse og lage falske utgaver. Sikkerhet er viktig! Ønsker ikke forfalskninger.
Iris autentisering
Iris skann og single sign on. Raskt, vanskelig å misbruke. Kan ikke mistes eller glemmes.
Ville foretrekke å bruke biometrisk autentisering om det fungerer optimalt. Ved hjelp av dette systemet slipper en å huske koder, passord og kort noe som jeg synes er et stort pluss.
Biometrisk. Lettere å misbruke vanlig autentisering.PIN-koder kan lett stjeles av uvedkommende.
Biometrisk sikkerhet er mer sikkert, i hvert fall inntil nå
Biometrisk autentisering. Enklere å bruke, pluss at du ikke får "lånt bort" din identitet.
Passord
Foreløpig vanlig passord. Enklere og mest brukt metode til nå. Har ikke særlig erfaring med annet.
29 fingeravtrykk, 8 øye, 1 enten øye eller fingeravtrykk, 4 biometriske opplysninger, og 2 passord. Totalt 44.
Fingeravtrykk: 66%, Øye biometri: 18%, Enten øye eller finger: 2%, Biometrisk autentisering: 9%, Passord: 4,5%.
Spørreskjema 2:
Fingeravtrykk - lett tilgjengelig, hygienisk, raskt
Fingeravtrykk hvis det fungerte hver gang. Greit å slippe å huske passord
Fingeravtrykk - enkelt
Fingeravtrykk eller passord
Fingeravtrykk. Har det med deg hver dag.
Fingeravtrykk ville jeg foretrukket fordi ikke to har like avtrykk. Kan ikke glemmes og vil være lettvint i bruk.
Fingeravtrykk eller håndgeometri. Da vil jeg slippe å huske å ta med id-kortet, eller stadig huske passord.
Kommer an på hvor sikkert systemet må være. Ved å blant annet kombinere to metoder som fingeravtrykk + ansiktsgjenkjenning (bilde) burde det bli ganske sikkert. Iris eller netthinne vil jeg tro er den sikreste metoden. Vanskeligst å kopiere. Men det er ikke trolig at dette er nødvendig for innlogging på datasystemet her. Da burde fingeravtrykk/passord være nok.

Iris
Øye eller fingeravtrykk
Øye. Regner med at det er ganske sikkert, raskt og enkelt.
Øye - virker vanskeligst å kopiere/misbruke.
Øye (iris eller netthinne) da dette virker mer sikkert
Øye eller fingeravtrykk
Øye
Øye? Vet ikke om det er fallgruver her. Fingeravtrykk i kombinasjon med passord/kode
Øye - har oppfattet at det er noe av det sikreste og det kan ikke "stjeles" fra meg. Trodde fingeravtrykk var sikrere enn det faktisk er.
Øye autentisering
Øye, da det er det sikreste systemet. Har det alltid tilgjengelig.
Biometrisk autentisering m/øye, fordi dette virker å være det sikreste pga. det er vanskelig å kopiere.
Øye. Lettvint, høres sikrere ut enn fingeravtrykk
Det virker enkelt i bruk med biometrisk autentisering men er litt usikker om noen kan stjele den, virker litt skummelt. Passord kan jo endres hvis det blir misbrukt, men etter hvert blir det mange passord å bruke
Jeg ville valgt biometrisk autentisering, da jeg har inntrykk av at det kan lette arbeidsdagen noe da vi bruker svært mange passord til vanlig. Men tviler litt på denne metoden da det er mulig å kopiere biometriske opplysninger. Hvor sikkert er det?
Biometrisk autentisering. Jeg tror det er sikrere enn å bruke passord/koder. Pluss at det er enklere å logge seg inn på data, låste dører og lignende.
Passord
Trodde fingeravtrykk var sikkert, men har endret mening. Vet ikke!
Id-kort + passord
8 fingeravtrykk, 12 øye, 3 biometrisk autentisering, 1 vet ikke, og 1 ID-kort + passord. Totalt 25.
Fingeravtrykk: 32%, Øye biometri: 48%, Biometrisk autentisering: 12%, Vet ikke: 4%, ID-kort+passord: 4%.

Questionnaire 1: 29 fingerprint, 8 eye biometrics, 1 eye or fingerprint, 4 biometric information, and 2 password. Total of 44.
Fingerprint: 66%, Eye biometrics: 18%, Eye or finger: 2%, Biometric authentication: 9%, Password: 4,5%.

Questionnaire 2: 8 fingerprint, 12 eye biometrics, 3 biometric information, 1 don’t know, og 1 ID-card + password. Total of 25.
Fingerprint: 32%, Eye biometrics: 48%, Biometric information: 12%, Don’t know: 4%, ID-card + password: 4%.