Security and usability assessment of several authentication technologies

Roar S. Sollie

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

In todays modern society, users have certain requirements to technology. They want to be able to access systems and perform tasks regardless of time and location. The problem that arises is how one can be sure that a person is the one he or she laims to be. Consequently, a secure validation of identity in an insecure environment is needed. This is usually performed by means of something the person is, has or knows.

The aim of this thesis is to determine if it is possible to combine different authentication methods, both biometrical and technical, and how this affects the security of the overall authentication routine. For example, an authentication procedure may include both password and a smart card. Security and usability of such a system is studied. One may also use two or more approaches from the same category, e.g. using face recognition and fingerprint, which both are in the category referred to as something one is. This thesis studies if the overall authentication system becomes stronger or weaker.

Keywords: multimodal authentication, biometric, smart card, fingerprint, usability, security metrics.

Sammendrag(Abstract in Norwegian)

I dagens samfunn har det blitt slik at man har endel krav til teknologien. Man ønsker å ha muligheten til å aksessere og utføre oppgaver og tjenester uavhengige av tid og sted. Problemene som da bringes frem er hvordan man kan være sikker på at en person er den han/hun utgir seg for å være. Hvordan kan man med sikkerhet validere om identiteten til en person er korrekt i usikre omgivelser? Er det mulig å implementere sikkerhetsrutiner som gjør at man med sikkerhet kan stadfeste en persons identitet? Autentisering og gjenkjenning av personer er mulig ved å benytte seg av noe man er, har eller vet.

Hensikten med denne masteroppgaven er å se om det er mulig å kombinere ulike autentiseringsmetoder, både biometriske såvel som tekniske, og hvordan dette eventuelt vil påvirke sikkerheten for autentiseringsrutinen. Bedres sikkerheten når autentiseringsmetoden inkluderer en kombinasjon av noe man er,har og vet, f.eks. et passord og smartkort, eller smartkort og fingeravtrykk. Hvordan vil i så tilfelle dette påvirke brukervennligheten? Man kan også benytte to eller flere metoder fra samme kategori, f.eks. ansiktsgjenkjenning og fingeravtrykk, hvilket begge er fra kategorien referert som noe man er, biometri. Vil dette gjøre autentiseringssystemet sterkere eller svakere?

Contents

Acknowledgments

A number of people have helped me making this work possible. My supervisor, Professor Slobodan Petrović, was very active and helpful in the guidance of this study. A co-worker at Buypass, Morten Johansen, programmed the application used in the experiment. Buypass AS, have lent me equipment, smart card readers and smart card, making it possible to conduct the experiment. Mads Henriksveen at Buypass has given me valuable feedback on this study from the very beginning. Thanks to Frode Volden, for the help on analysing the experimental data.

I could not have performed the experiment without the participants. Thanks to them for lending me their fingerprints and valuable time.

1 Introduction

This chapter contains a description of the problem identified in this thesis and the research questions, as well as motivation, justification and benefits.

1.1 Problem description

Traditional authentication methods, for example traditional passwords, PIN-code or question-and-answer, sometimes suffer from known and exploitable weaknesses. A password is something one ought to remember, and is often based on words, which can be guessed easily. PIN-codes are seldom longer than four digits, which makes them easy for an adversary to guess if there is no mechanism to control the number of attempts. Stronger authentication methods, e.g. smart cards, fingerprints, iris patterns and face recognition, also suffer from some known weaknesses. This is mostly because the authentication takes place in an insecure environment.

This thesis deals with security of a combination of two or more authentication methods. A set of metrics for evaluating usability and security of various authentication methods has been defined. Combinations that lead to the strongest security of the overall authentication system are determined. The relation of security and usability of such combinations is also studied.

1.2 Justification, motivation and benefits

Verification of the identity of a person is important, having in mind the possibility of theft and fraud of both money and identity. If security is compromised, privacy is likely to be compromised as well. The whole information environment is based on trust. Stakeholders for such knowledge and information would be those that need strong authentication methods and other people interested in authentication.

Implementation of strong authentication methods is important in the strategy of securing information, especially in organisations in which it is critical for the information security that no unauthorized entities gain access to these information systems. In systems with information regarding money transactions and sensitive personal information, it is critical to have strong authentication methods in order to assure protection against fraud and unauthorized use or leakage of information. The dilemma however is whether the level of security affects the overall usability of the system.

1.3 Research questions

- How is security affected by combining two or more authentication methods?
- To what extent the security affects the level of user-friendliness? How does a combination of authentication methods affect this issue?
- Is it reasonable to implement a combination of two or more authentication methods?

1.4 Research method

A qualitative method seems to be appropriate for answering the research questions. In [1] it is described that the goal of the qualitative method is to gain a deeper understanding of the problem complexity. [2] provides additional information about the choice of method and describes the work from formulating questions to seeking and finding solutions.

A literature study has been performed in order to gain information and knowledge about the various authentication methods and the environment in which they are implemented. The purpose of this literature study was to be able to make some conclusions about the strength of different methods and to be able to evaluate authentication methods according to security and usability.

An experiment has been conducted mainly in order to try to compare the perceived security and usability with the actual security. The security and usability have been measured according to a set of metrics defined as a result of the literuature study. It is important to normalize these metrics, making it possible to compare the results from different authentication methods. The aim of the experiment was to contribute to an estimate and comparison of the level of security when the different methods of authentication are combined. The experiment was focused on the use of smart cards, username and passwords, and fingerprint. One of the important issues is the time of execution and effort needed to perform the authentication procedure, and to which extent this affects the usability and user-friendliness. The experiment helps answering the research questions and acts as a basis for the conclusions.

2 Previous work

This chapter contains a literature survey of research in this area related to the research questions stated in Section 1.3.

2.1 Review of different authentication methods

Ordinary (unimodal) authentication methods have been studied extensively in order to estimate the level of security that can be achieved with them.

In [3], several authentication methods are described, as well as advantages and disadvantages of those methods. The paper [3] can therefore be referred to as a well-describing basic paper for people interested in authentication research. Chun [3] concludes that passwords should be replaced, and that smart cards with digital signatures will increase rapidly in use. Chun also believes that biometrics are unlikely to be implemented for reasons of cost, data storage, processing time, ergonomics and ethical issues.

[4] refers to how secure smart cards are, their potential vulnerabilities, their security and presents a cost/benefit analysis of their application. The paper [4] is therefore used as an important reference in the work regarding smart cards in this thesis. Abbott [4] states that smart cards are very secure, but that there are some known vulnerabilities. However, these vulnerabilities require extensive technical expertise and very expensive equipment in order to be exploited. Smart cards can provide an additional level of security and help reduce risks in existing systems.

In [5], threats for smart cards are described and a security model of a smart card system is discussed independently of its application. A trust environment is modelled as well as all potential parties involved in any smart card system: the cardholder, the terminal, the data owner, the card issuer, the card manufacturer, and the software manufacturer.

In [6], many important issues, related to the research questions, are discussed. These include for example: ease of use, applicability, speed of verification, vulnerability to fraud, size of storage and multiple authentication technologies. This book explains the basic concepts of biometrics and biometric technologies, as well as their applications in the electronic world.

The master thesis [7] studies the disadvantages of using face recognition in electonic passports. The purpose of biometric passports is to prevent the illegal entry of travellers into a specific country and limit the use of counterfeit documents by more accurate identification of an individual. [7] states that there is a great deal of risk for identity theft using only one biometric authentication in a passport.

In [8] many of the biometric authentication methods available are addressed and their usability and security according to strengths, weaknesses and cultural concerns are discussed. It concludes that: "*Biometrics offers at least in part a way to defend against cyber terrorism and provide increased network security*".

In [9], the problems of authentication have been discussed, and the uncertainty inherent to authentication decisions has been emphasised. It concludes that experience is needed to determine exactly how to best realize authentication confidences in practice.

In 1994 NIST published FIPS 190 [10], a guideline describing the primary alternative methods for verifying the identities of computer system users. It states that single password authentication systems are too weak, and that one should use passwords, tokens, and biometrics in different combinations to achieve better assurance in the authentication system.

2.2 Comparison of various authentication methods. Security of a combination of two or more authentication methods

Since unimodal authentication does not offer satisfactory security, various efforts have been invested in studying multimodal authentication methods.

In [11], it is discussed how the combination of smart card and biometric authentication, e.g. fingerprint, affects security. [11] also compares the level of security achieved in such a system with the traditional PIN authentication system.

[12] describes how combining several biometric authentication methods improves the accuracy and decreases false-positives and false-negatives to the level which cannot be achieved with a single-model biometric solution. It states that one can use two techniques to increase the reliability of biometric authentication: multiple samples and multiple biometric sources.

[13] discusses and compares usability between the password authentication method and other authentication methods, for example pass faces. It also takes into consideration that token-based biometric, and other authentication methods, often require special and expensive hardware. [13] states that the use of passfaces showed a third of the login failure rate of passwords, despite the fact that the users had a third of the frequency of use.

[14] evaluates authentication with the use of biometrics and proposes a classification of biometric authentication systems. This classification helps comparing different biometric authentication systems. If one removes the liveness characteristic, this classification could also be used to evaluate other authentication systems. [14] also discusses advantages and disadvantages of biometrics, and where not to use biometrics. It is concluded that a system containing cryptographic functions, biometric matching, feature extraction and the biometric sensor in one tamper-resistant device would be ideal. Biometric is a good add-on authentication method, but not a basic one. Even cheap and simple biometric solutions may increase the overall system security when combined with an existing authentication method.

[15] develops an approach to evaluation of the security of computer systems using vulnerabilities represented in a privilege graph. Privelege graph consists of nodes with weighted archs, where the nodes are systems or resources and attackers. The weight of each arch corresponds to the probability and seriousness of the attack. A security breach can occur if there exists a path between a node representing a possible attacker to a node representing an attack target. Three intuitive properties can be derived from this example:

1. Security increases if the "length of the paths" leading to the target increases.
2. Security decreases if the "number of paths" leading to the target increases.
3. Security is mainly affected by the shortest path leading to the target.

[15] states that "Security is directly proportional to the time needed by an attacker to succeed in his attack".

In [16], the integration of two biometric techniques, voice and face recognition, as well as the potential benefit of combining these techniques in order to improve the robustness of person identification is studied. It is concluded that the combination of these techniques is capable of identifying persons with high accuracy under tightly constrained conditions. In addition to face and speech recognition, [17] combines these with observing lip motions. The results of this study show that the integration of two or three techniques leads to better recognition rates.

Various authentication methods are described in many more articles and papers. For example, [18] considers hash visualization in user authentication, and a prototype where a user is authenticated by recognizing a set of previously seen images has been described. In [19], the same problem as in [18] is analyzed in more detail. [19] concludes that since the error recovery rate was significantly higher for images, compared to passwords and PINS, such a system may be useful in environments where high availability of a password is paramount and where the difficulty to communicate passwords to others is desired.

[20] describes various authentication methods: password, token and biometric authentication. It compares weaknesses and strengths of different authenticators and states that human authentication is a critical concern for corporate security. [20] also provides insight into advantages and disadvantages of current options.

[21] and [22] provide an excellent overview of personal authentication mechanisms. [21] discusses biometrics and different characteristics that make them usable. Characteristics mentioned are uniqueness, universality, permanence, user-friendliness, cost and accuracy. It also discusses advantages and problems of using biometric identification. [22] provides an overview of authentication, and discusses the problem of verifying identities and how to make it work properly. It mentions both authentication methods as well as vulnerabilities and types of attacks.

[23] takes advantage of the capabilities of each individual biometric, to overcome both the speed and the accuracy limitations of a single biometrics in performing personal identification. It considers a number of issues related to designing a multimodal biometric system: the main purpose of utilizing multiple biometrics, the operational mode, which biometrics should be integrated and the sufficient number of biometrics.

[24] states that the smart card plays an important role as security tool, and disusses the advantage of using a biometric instead of a knowledge based password or PIN as a verification method. To rule out security threats regarding offcard-matching, the biometric matching algorithm has to be implemented in the smart card to avoid carrying out the data matching in a separate device. Biometric is accepted not only as an add-on method but also as an adequate alternative to knowledge based authentication if the biometric components reach the strength of function "high" according to the ITSEC[1] evaluation criteria [25]. Even if an attacker possesses someone else's smart card, a terminal with the biometric module and the user's verification data, he cannot successfully present the verification data to the smart card.

[26] discusses the fact that it is desirable and feasible to implement on-card matching algortihms, allowing to perform biometric user verification in the smart card. If a smart card provides functions such as electronic signature creation, electronic money and/or

[1] ITSEC, Information Technology Security Evaluation Criteria

sensitive data such as medical data, then the smart card has to verify that it is used by the legitimate card holder.

[27] describes different biometric technologies and evaluates them according to the desirable properties described in more detail in Section 3.3.1 and Table 1 in this thesis.

Short description of the biometrics evaluated in [27] are:

- *DNA*: DeoxyriboNucleic Acid. The ultimate unique code for one's identity. Its drawback is that verification of the DNA markers needs laboratory equipment and cannot be done by the customer or consumer themselves.
- *Ear*: The shape of the ear. Not expected to be sufficiently unique.
- *Face*: One of the most accepted biometrics. Affected by aging, facial expressions, environment variations etc.
- *Facial, hand, and hand vein thermogram*: The pattern of the heat radiated by the body. A facial thermogram can also be captured in poorly lit environments. Research has not yet determined if facial thermograms are adequately discriminative, e.g. they may depend heavily on the emotion or body temperature of an individual at the moment the scan is created [28].
- *Gait*: The peculiar way one walks. Behavioral and may not stay invariant.
- *Hand and finger geometry*: Features related to human hand, e.g. length of fingers.
- *Iris*: Visual texture of the human iris. Distinctive for each person and each eye. One drawback is that the user must look directly into the retinal reader. This is inconvenient for eyeglass wearers.
- *Retinal scan*: The retinal vasculature is rich in structure, and is distinctive for each person and each eye. One drawback is that the user must look directly into the retinal reader. This is inconvenient for eyeglass wearers.
- *Keystroke dynamics*: There is a hypothesis that each person types on a keyboard in a characteristic way. Behavioral, influenced by injuries, sickness and emotions.
- *Odor*: Each person odors a chemical characteristic. Affected by environment, type of food eaten, deodorant used etc.
- *Signature*: The way a person signs his/her name. Behavioral, influenced by emotions and may change over time. Behavioral, influenced by injuries, sickness and emotions.
- *Voice*: Voice capture is unobtrusive and an acceptable biometric. One problem is mimicking.

The biometrics described above are compared in Table 1. Fingerprint recognition has a very good balance of all the desirable properties. Fingerprints have a long history of use in criminal investigation, they have a stigma or negative characteristic associated with them. Biometric Market Report (International Biometric Group) estimated the revenue of various biometrics in the year 2002 and showed that fingerprint-based biometric systems continue to be the leading technology in terms of market share, covering more than 50% of non-AFIS[2] biometric revenue.

[2]AFIS- automatic fingerprint identification system

Biometric identifier	Universiality	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	L	L	M	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 1: Comparison of biometric technologies. High, Medium and Low are denoted by H,M, and L, respectively[27].

Biometrics to enchance smart card security are discussed in [11, 29]. Smart cards are normally used as a secure and tamper-proof device to store sensitive information such as digital certificates, private keys and personal information. PIN code has been the usual way to access the information on the smart card. Research and experience shows that PINs are weak secrets in the sense that they are often poorly chosen and easy to loose and lend away. Biometric authentication with smart card has been proposed by matching a stored biometric template to a live biometric template [8, 29, 30]. Related to introducing biometric authentication in combination with smart card, three strategies of the biometric authentication can be identified [11]:

1. Template on Card(TOC: the biometric template is stored on a smart card and the matching with the live template is performed on a computer or a device using a microprocessor.
2. Match on Card(MOC): the biometric template is stored on a smart card which also performs the matching with the live template.
3. System on Card(SOC): a combination of the previous two technologies. The template is stored on a smart card which also performs the matching. The biometric scanner or device is hosted on the smart card.

Defining security metrics for a combination of authentication methods has not been addressed in the literature. However, we consider this problem significant, since there is no guarantee that combining various authentication methods actually increases the security level of the overall system. We have defined metrics for this purpose and evaluated them for several combinations of authentication methods. The definitions of the metrics are given in Chapter 3.

2.3 Security vs. user friendliness in a combination of authentication methods

In [31] the complications when attempting to create a secure pervasive computing environment are explored. It discusses challenges in both physical and information security, and the fact that authorisation, auditing and non-repudiation all rely on an accurate identification and verification of the user.

[32] describes different aspects of authentication, the issue of authentication and privacy, and the issue of security and usability. One of the crucial factors that encourages or discourages the use of any authentication technology is ease of deployment. A scheme that relies on something that users already have (or already "are") is easier to deploy than the one that requires shipping (and perhaps installing) new equipment.

In [33], the issues of usability, acceptability and privacy in the biometric authentication environment are discussed. The sensors are getting smaller, cheaper, more reliable, and designed with better ergonomic characteristics. The biometric algorithms are also getting better, and many systems include features to train the users and provide feedback during the exploitation. This may improve usability and acceptability of biometric applications.

[14] and [27] describe usability of biometric authentication methods and discuss central issues regarding failure to enrol (FTE), false acceptance rate (FAR) and false rejection rate (FRR). [14] also lists a set of parameters for biometric systems and proposes a classification of biometric systems. It states that solutions where the cryptographic functions as well as the biometric matching, feature extraction and biometric sensor are all integrated in one tamper resistant device are promising. The authors of [14] also believe that biometric authentication is a good additional authentication method, increasing the overall system security if used on top of existing traditional methods.

[27] concludes with a set of desirable properties in fingerprint scanners:

- automatic finger detection
- automatic fingerprint capture
- temporary storage of captured fingerprint image
- vitality or liveness detection
- compression of the image
- matching of the fingerprint on the sensor
- inclusion of a smart card reader or template database storage
- cryptographic security protocols implemented in the scanner to carry out secure communication

[34] explores the requirements and development methods for user-centered security. Usability and security must be merged in order to produce acceptable systems that will not be circumvented by the legal or non-legal users.

When authentication techologies are combined, additional security factors work in cooperation so the need for highest-level FAR may no longer be necessary [35]. Smart cards combined with a biometric offer a number of advantages. Providing the template at the biometric device removes any storage limitation on the device or a need for access

to a central repository. The smart card also offers a level of tamper resistance. [35] also discusses the multifactor authentication solution combining biometrics with smart cards and public-key infrastructure (PKI), that adds an extra layer of security with cryptography. PKI is mathematically more secure than biometrics and it can be used over the Internet.

2.4 Overall evaluation of a combination of two or more authentication methods

In [36], the problems of measuring information security and identifying good authentication practises have been discussed. The goals were to characterize the information security measurement problem, identify good practices and focus needs.

There are several articles, e.g. [4] and [13], bringing up the cost/benefit-question when different authentication methods are evaluated. [4] concludes that organisations, implicitly or explicitly, make decisions based on whether the cost of the decisions is justified by the benefit, and that these determinations are often more subjective than objective. If the cost of the new feature is less than the value of the reduced risk plus any additional benefits provided by the card, then the device should be implemented.

In [37], it is stated that an employee is most likely to forget his/her password four times in a year on average. When the cost of resetting a password is applied to thousands of employees it becomes astronomical. [37] also concludes that when implementing a biometric authentication system, companies must be economically aware that as the required level of authentication increases, so does the cost.

3 Metrics for assessing security and usability of authentication systems

In order to have an evaluation of the security and usability, metrics are well-organized tools to help measure these values. Section 3.1 defines the template used when defining the metrics, both for security and usability. In Section 3.2 and 3.4 the criteria regarding security and usability are discussed, resulting in the metrics defined in Section 3.3 and 3.5.

3.1 Metric template

When defining the metrics, the template defined in [38] was used and the results from [39] were studied. The metrics are by no means meant to be a complete guide, but they may contribute to identify and define some of the major problems. A modification on the template given in [38] was made by adding reliability and validity to help measuring the completeness and correctness of the metrics. The template metric is presented in Table 2.

Metric ID	**The unique identifier of current metric.**
Name	Name of the metric (short form).
Performance Goal	Measure and see if objectives and/or techniques stated by the metric are implemented.
Performance Objective	Description of actions required to accomplish the performance goal.
Metric	Description of what we are measuring with this metric.
Purpose	The goal of this metric.
Implementation Evidence	Tasks and subquestion to help measuring the critical element.
Frequency	How often the metric is conducted.
Formula	Describes the calculation performed. Assessed as a quantitative result.
Data Source	The data used to perform the metric.
Indicator	What this metric is trying to present.
Reliability	The possibility for incidental and random errors performed by this metric [40].
Validity	The fact that we measure the purpose of the metric [40].

Table 2: Template defining a security metric

3.2 Security criteria

[14] discusses advantages and disadvantages of biometric authentication systems and proposes a classification of such systems making it possible to compare the biometric systems reasonably. It also lists a set of parameters used for evaluating differences among various authentication systems. The fact that fingerprints are tested, makes these parameters usable when evaluating the different authentication systems. The parameters have been modified and are listed below:

Liveness testing:

- Measures whether or not the biomteric is from a living person, e.g. blood circulation, more information in Section 3.3.1.
- Makes the attack more difficult. A combination of multiple liveness tests can make the system more secure.
- Scale: *no*, *yes* or *multiple*

Tamper resistance:

- Without tamper resistance or supervision the system can be tampered with and forged/replied biometric data can be injected into the system.
- Scale: *no*, *moderate* or *advanced*

Secure communication:

- The communication among modules within a tamper-resistant cover need not be secured, but the communication over an insecure line should be authenticated and encrypted.
- Scale: *no* or *yes*
  - If *Yes*; the length of the encryption key indicates the level of security using the specified algorithm.

Traditional authentication:

- The authors of [14] refer to traditional authentication as something one knows (e.g. PIN or password) and/or has (e.g. smart card, key or passport).
- Scale: *sufficient/not sufficient*, *any time*, *required* and/or *malfunction*

[14] evaluates the "secure communication"-parameter using yes or no answers. When using a secure communication, authentication and/or encryption, it is useful to assign a weight to the "yes"-alternative according to the length of keys used. The fact that the key is long does not guarantee security, but if it is short it is obvious that such a system is insecure.

By evaluating the systems using these parameters, a classification of the systems can be done. [14] proposes four different levels, listed in Table 3 and described in more details below.

Level 1: Very simple systems

- No tamper resistance: offer restricted security and are easily evaded (unplugging the device or injection of previous eavesdropping information).
- Communication among modules need not be encrypted nor authenticated.

Level	Liveness	Tamper resistant	Secure communication	Traditional authentication
1	no	no	no	sufficient/any time
2	no	no	no	sufficient/malfunction
3	yes	moderate	yes/score	not sufficient
4	multiple	advanced	yes/score	not sufficient/required

Table 3: Level of security-classification

- No liveness test: successful biometric authentication is a sufficient mean of authentication.

Level 2: Simple systems

- No tamper resistance: the easiest attacks are eliminated, but can be tampered with, by e.g. fake biometrics.
- Require mutual authentication and encrypted communication.
- Some level of security, but still low.
- Traditional authentication is offered as sufficient authentication in cases of malfunctions.

Level 3: Intermediate systems

- Exposed components must be guarded or tamper resistant; resistant to moderate attacks. Advanced tampering/artificial biometrics are able to evade the system.
- Some kind of liveness testing.
- Communication must be mutually authenticated and encrypted.
- The system never offers traditional authentication as a sufficient method.

Level 4: Advanced systems

- Advanced (multiple) liveness test.
- Exposed and un-guarded components must be tamper resistant. Able to resist advanced tampering attacks.
- Communication must be authenticated and encrypted, except within a tamper resistant box.
- A supplemental traditional authentication method is necessary.
- Resist professional/advanced/well-founded attacks
- Note: "There is no 'ideal solution' for security [41]".

In addition to these criteria, an important value to measure is the use of multiple authentication and if the auhtentication methods used are from different categories: *knows*, *has* and/or *is*. An authentication system that relies on multiple authentication methods leads to security improvement [11, 12, 16, 24].

3.3 Metrics for security

A statement often referred to in the literature is due to Dacier, Deswarte and Kaaniche [15]: "*Security is directly proportional to the effort required for the implementation of an attack.*".

3.3.1 Liveness testing

Liveness testing relies on the use of a biometric feature. Any human physiological and/ or behavioral characteristic can be used as biometric a identifier to recognize a person as long as it satisfies a set of requirements [27, 42]:

- universality, meaning that every person should have the biometric.
- distinctiveness, meaning that any two persons should be sufficiently different as to their biometric features.
- permanence, meaning that the biometric should be sufficiently invariant.
- collectability, indicates that the biometris can be measured quantitatively.

In addition to these, there are a number of other properties that should be considered, e.g.:

- performance, which refers to recognition accuracy, speed, robustness, resources needed to achieve these issues, and operational and/or environmental factors affecting the accuracy. These factors are discussed in more details in Chapter 3.4.
- acceptability, refering to privacy issues and the fact that people are willing to accept a particular biometric identifier in their daily lives.
- circumvention, reflects the effort needed to evade the system [15].

Table 4 is a metric measuring whether or not liveness testing is present in current authentication system.

3.3.2 Tamper resistance

Tamper resistance includes protection against different types of attacks, refered to as side channel attacks. Side channel attacks are described in [43] and [44] and include:

- Probing attacks
- Fault induction attacks
- Timing attacks
- Power analysis attacks
- Electromagnetic analysis attacks.

Probing attacks involve depackaging the smart card and observing its behavior by attaching wires to the data bus or by observing the memory cells directly with a microscope.

[44] defines fault induction attacks as, "tampering with a device in order to have it perform some erroneous operations, hoping the result of that erroneous behavior will leak information about the secret parameters involved".

Timing attacks exploits the running time of cryptographic operations to deduce the secret information.

Metric ID	**SM-1**
Name	Liveness testing
Performance Goal	If the system uses biometric authentication: determine whether or not it has a liveness test.
Performance Objective	Are effective mechanisms implemented to detect whether or not the biometric is from a living person or an artificial biometric?
Metric	If there is a liveness detection implemented or not.
Purpose	To see if the fingerprint reader has mechanisms making it able to separate an artificial finger or fingerprint from a real finger or fingerprint.
Implementation Evidence	1. Does the system use biometric authentication? No[ ] Yes[ ] If Yes. which type(s): _____ _____ 2. Does the system have liveness testing? No[ ] Yes[ ] Multiple[ ] If Yes. which type(s): 1. UV(blood circulation) [ ] 2. Sweat glands [ ] 3. Temperature [ ]
Frequency	Once.
Formula	1 point if it uses biometric, 1 point if it have liveness testing and 2 if it has multiple liveness testing.
Data Source	Manual and information about the system/device.
Indicator	This metric presents how robust the device is against attacks with artificial fingers/fingerprints.
Reliability	There is no way of knowing how the fingerprint acts on new and better artificial fingers and/or fingerprints.
Validity	It is not for sure that the liveness test is of good quality, the way it is stated.

Table 4: Liveness metric

[45] examines power analysis attacks on smart cards, and [46] announced an attack against smart card microprocessors. By monitoring the power consumption of a smart card, they reported that it was possible to extract the secret key of an executing cryptographic algorithm. In [46] and [47] Kocher et al. state that virtually all smart cards were vulnerable to these attacks.

Electromagnetic analysis attacks exploits correlations between electromagnetic emanation and internal secret information.

The security metric measuring tamper resistance is shown in Table 5.

Metric ID	**SM-2**
Name	Tamper resistance
Performance Goal	Measure how tamper resistant the authentication system is.
Performance Objective	Determine if there are effective mechanisms implemented to avoid tampering.
Metric	Is or to which degree is the authentication system/device tamper resistant.
Purpose	To see if the system/device has protection against tampering attempts and if forged/replied biometric data can be injected into the system.
Implementation Evidence	Is the system/device tamper resistant, and to which degree? No[ ] Moderate[ ] Advanced[ ] If tamper resistant, which type(s) of attacks is it protected against: 1. Probing attacks [ ] 2. Fault induction attacks [ ] 3. Timing attacks [ ] 4. Power analysis [ ] 5. Electromagnetic analysis [ ]
Frequency	Once
Formula	Scoreboard where no=0, moderate=1 and advanced=2.
Data Source	Manual and information about the device.
Indicator	This metric presents how robust the system or device is against tampering and injection of forged or replied biometric data.
Reliability	There is no way of knowing how or if an attacker will succeed in the future, but for now the test should be reliable.
Validity	It is not for sure that the information found about the device is correct.

Table 5: Metric for measuring tamper resistance.

3.3.3 Secure communication

The communication among modules within a tamper-resistant environment need not be secured, and the communication over an insecure line should be authenticated and encrypted. The effectiveness of this protection depends on a variety of parameters, such as cryptographic key size [48], protocol design and password selection.

According to the study and conclusions made in [48], the recommended lower bounds for computationally equivalent key sizes for year 2005 are presented in Table 6. In commercial applications, one often has to make guaranties for the confidentiality and integrity for the next 20 years, therefore recommended key sizes for 2025 as upper bounds have been used, which gives the maximum score. In Table 6, SDL is a short for subgroup discrete logarithm systems and elliptic curve cryptography systems are shorted ECC. Data Encryption Standard (DES), triple DES (3DES) and the Advanced Encryption Standard (AES) are examples of symmetric block ciphers. Examples of asymmetric or public-key cryptography algorithms are RSA, digital signature standard (DSS) and Diffie-Hellman (DH). The recommended key sizes in Table 6 have been adjusted according to the number of bytes, making them divisible by eight. Table 7 shows the number of scores that

belong to the different encryption key sizes.

Year	Symmetric key size	Asymmetric key size	SDL key size	ECC key size
1990	63	622	112	117
2005	74	1149	131	139
2025	89	2174	158	169

Table 6: Lower bounds for computationally equivalent key sizes (in bits) in 1990, 2005 and 2025 [48].

Points	Symmetric key size	Asymmetric key size	SDL key size	ECC key size
0	0	0	0	0
1	0-64	0-624	0-112	0-120
2	64-80	624-1152	112-136	120-144
3	80-96	1152-2176	136-160	144-176
4	>96	>2176	>160	>176

Table 7: Score table (in bits).

The secure communication metric, shown in Table 8, measures whether or not the communication is authenticated and/or encrypted.

We do not evaluate the algorithms as to strict mathematics, if the algorithms are too complicated or implemented well. We have to assume that this has been done properly according to the standards and documentation.

Pitfalls regarding the cryptographic algorithms are discoverd on daily basis, and there will always be unknown pitfalls. Asymmetric cryptographic keys with size up to 512 bits have been factorized by non-military organizations, indirectly meaning that military organizations or organizations with large funds available have been able to factorize larger keys. This means that one has to choose larger keys (stronger security) than what is supposed or said to be strong enough [48].

Even if the encryption is sufficiently strong, the environment and encapsulation of data have to be secure. [26] states that evaluation of the system according to ITSEC [25] or Common Criteria [49] is required. The evaluation assurance level depends e.g. on the quality of the electronic signature which will be created by the respective card. If the signature creation data is protected by biometric user verification, then the respective biometric verification method is also subject to evaluation. In UK a "Biometric Device Protection Profile"[50] is under development, and is supposed to help in evaluation and testing of biometric devices.

3.3.4 Traditional authentication/Fall-back mode

Traditional authentication is refered to as something one knows or has, e.g. PIN, passwords, smart card, key or passport. In addition, an authentication system may offer traditional authentication, because:

- it is sufficient and therefore offered as method of authentication at any time.
- additional methods like e.g. something one has, or a biometric method, is needed as a secondary solution.

Metric ID	**SM-3**
Name	Secure communication
Performance Goal	Determine if there are mechanisms implemented to avoid tampering.
Performance Objective	See whether or not the communication is secured. Communication in an insecure environment should be authenticated and/or encrypted.
Metric	Does the system have a secured communication channel/line and to which extent are the algorithms good and length of keys sufficiently large.
Purpose	To see if the communication in an insecure environment are secured properly, using authentication and encryption.
Implementation Evidence	Is the communication secured, using authentication and/or encryption? No[ ] Authentication[ ] Encryption[ ] Both[ ] If secured: -type of algortihm _____ -size of key _____
Frequency	Once
Formula	1 point if the communication is authenticated and encrypted, 0-4 points depending on the size of the key (4 points if the key is equal or larger then the upper bound, see Table 7).
Data Source	Manual and information about the system/device and information about recommended key sizes on the employed algorithm..
Indicator	Presents the overall security on the system and its communication. Secure communication is an important key criterion of good security.
Reliability	Score for different algorithms and size of encryption keys may be somewhat subjective.
Validity	Will give an indication on whether or not the communication is secured.

Table 8: Metric for measuring secure communication

- it may be required that the system supports traditional authentication, e.g. in cases of malfunctioned persons, also refered to as fall-back mode.

[26] lists cases where biometric methods are neither suitable nor applicable to any user:

- rejection due to personal reasons
- cultural incompatibility
- absence of the respective biometric feature
- insufficient characteristics of the respective biometric feature
- abnormal characteristics of the respective biometric feature

Therefore one should always expect that the knowledge based user verification method will be available as an alternative method. In cases where the user wants and has the possibility to use biomterics, the PIN or password will remain as a backup possibility.

The metric measuring these issues is shown in Table 9.

Metric ID	**SM-4**.
Name	Traditional authentication
Performance Goal	State whether the system offers a traditional authentication method, and when it is used.
Performance Objective	If the system relies on biometric authentication, not everyone have the opportunity to enrol because of malfunctionality, injuries or sickness. The system should therefore offer a fall-back mode using e.g. PIN, password or smartcard.
Metric	Does the system rely on traditional authentication alone or does it offer any fall-back mode when using biometric authentication.
Purpose	To measure if the system offers a fall-back mode when using biometric authentication and to see whether the system relies on non-biometric authentication.
Implementation Evidence	1.Does the system use biometric authentication? No[ ] Yes[ ] If Yes: 1a.Does the system require a fall-back mode? Not required[ ] Required[ ] 1b.Are non-biometric authentication sufficient? Not sufficient[ ] Sufficient[ ] 1c.When to use/offer fall-back mode? Not at all[ ] Malfunction(FTE/FTA)[ ] Anytime[ ]
Frequency	Once
Formula	Score:1 point if fall-back mode is required, 1 point if traditional authentication is no sufficient enough and 1 point if fall-back mode is offered only in cases of malfunctionality.
Data Source	Security policy of the system, manual and other information about the system/device.
Indicator	Presents a score on security issues and complexity of the system.
Reliability	The use of fall-back mode may defer and subjective decisions may introduce weaknesses in the system.
Validity	The metric is valid because it measures the use and existence of fall-back mode, and use of traditional authentication.

Table 9: Metric for use and evaluation of traditional authentication

3.3.5 Multiple authentication

The use of multiple authentication brings security in both depth and width. Authentication in width in this context refers to the use of two or more authentication methods from the different authentication categories: *knows*, *is* and/or *has*. One example is smartcard with PIN, where the smart card is a token one has, and the PIN is something one knows. Authentication in depth is if one uses two or more authentication methods from the same category, i.e. password and PIN from the *knows* category. The metric measuring multiple authentication is shown in Table 10.

Metric ID	**SM-5**.
Name	Multiple authentication
Performance Goal	State whether the system uses multiple authentication methods.
Performance Objective	A system should not rely on one single authentication method. The system should include more than one, ideal is perhaps one from each category: *knows*, *is* and *has*.
Metric	Does the system use multiple authentication methods.
Purpose	To measure how many authentication methods are used, authentication in depth and width.
Implementation Evidence	1.Does the system use multiple authentication methods? - No[ ] Yes[ ] Multiple[ ] If Yes: -How many?_____ 2.From which categories of authentication are the method(s) used? - Knows[ ] Is[ ] Has[ ]
Frequency	Once
Formula	1 point for each authentication method used, 0 points if one category is used, 2 points if two categories and 4 if all three categories are used.
Data Source	Information about the system.
Indicator	Presents a score on security in depth and width.
Reliability	The use of multiple authentication may introduce security in depth and width.
Validity	The metric is valid because it measures level of security presented by the number of authentication methods combined.

Table 10: Metric for use and evaluation of multiple authentication methods.

3.4 Usability criteria

Usability of an authentication system is strongly related to speed and accuracy. If the authentication system is too slow in the process of evaluation and verification of the user, it will not be successful. The usability can be affected by many factors. According to [34], some of the factors may be:

- Time to learn
- Speed of performance
- Subjective satisfaction
- Rate of errors by users

In addition to these, the following parameters have been added:

- Rate of errors by the system

Rate of errors by users and/or by the system will affect the accuracy of the system. A biometric verification system makes two types of errors[51, 27]:

i. mistaking biometric measurements from two different persons to be from the same person, called false match (FM).

ii. mistaking two biometric measurements from the same person to be from two different persons, called false non-match (FNM).

There is a trade-off between false match rate (FMR) and false non-match rate (FNMR) in every biometric system. Both FMR and FNMR are functions of the system treshold t. If t is decreased to make the system more tolerant to input variations and noise, then FMR increases, and if t is raised to make the system more secure, then FNMR increases accordingly, Figure 1.

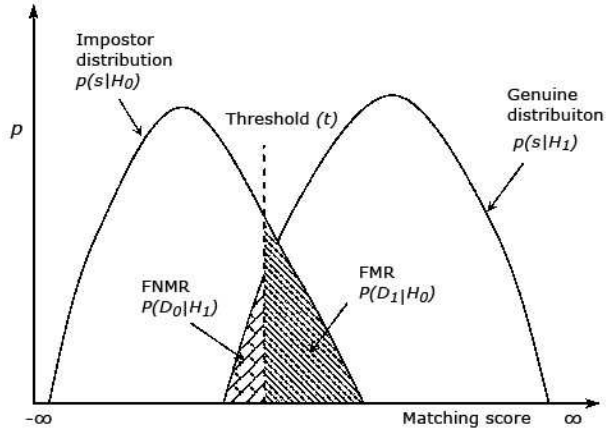

Figure 1: Biometric system error rates.

In 1 the null and alternate hypotheses are:

H_0: input does not come from the same person as the template.

H_1: input comes from the same person as the template.

The associated decisions are:

D_0: the person is not who he/she claims to be.

D_1: the person is who he/she claims to be.

3.5 Metrics for usability

3.5.1 Time to learn

The learning phase affects both the cost of implementing the system and to gain acceptance among the users. If the learning phase requires a lot of time and patience, it is not certain that the users, often employees, are willing to use the system. This will make the implementation of the system a waste, and a lot of time and money may be lost. Effort is strongly related to the time consumption, and the subjective opinion of the effort needed is more easily measured.

The metric measuring the learning phase is shown in Table 11.

Metric ID	**UM-1**
Name	Time and effort to learn
Performance Goal	Measure the effort it takes to learn and get comfortable using the authentication system.
Performance Objective	Determine the effort used for a new user to learn how the system works, the enrolment and how to use the system.
Metric	Effort of the learning phase.
Purpose	To measure the effort needed to learn be comfortable with the authentication system.
Implementation Evidence	Measure the users opinion of the time to learn and use the authentication system. No problem 5[ ] 4[ ] 3[ ] 2[ ] 1[ ] Difficult
Frequency	Once pr person/user.
Formula	Points given according to the implementation evidence.
Data Source	The participants opinions.
Indicator	One of many factors affecting the usability of the authentication system.
Reliability	The effort needed to learn depends on the level of knowledge of the user. Using >30 test persons will strengthen statistical reliability of the results.
Validity	The validity for this metric is very good.

Table 11: Metric for evaluation of time and effort needed to learn the authentication system.

3.5.2 Speed of performance

The speed of performance is closely related to the concept of acceptable time of use. Users are getting critical to the use of a system if it takes to much effort and time.

The speed of performance metric is shown in Table 12.

<table>
<tr><td>Metric ID</td><td>UM-2</td></tr>
<tr><td>Name</td><td>Speed of performance</td></tr>
<tr><td>Performance Goal</td><td>Measure acceptable time consumption during the authentication phase.</td></tr>
<tr><td>Performance Objective</td><td>After the learning phase, it is important to determine the time of use when performing the authentication. It is critical that the authentication does not take excessive amount of time.</td></tr>
<tr><td>Metric</td><td>Time consumption of the authentication phase.</td></tr>
<tr><td>Purpose</td><td>To measure the time of use during the authentication process, using current authentication system.</td></tr>
<tr><td>Implementation Evidence</td><td>Measure the time of use during the authentication phase (in seconds).
_____</td></tr>
<tr><td>Frequency</td><td>Once pr person/user. Depending on the available time, it may be of interest to perform several measurements. One day/week/month after the enrolment.</td></tr>
<tr><td>Formula</td><td>Average time used (in seconds).
<table>
<tr><td>Points</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td></tr>
<tr><td>Time in seconds</td><td><10</td><td>10-15</td><td>15-20</td><td>20-25</td><td>>25</td></tr>
</table></td></tr>
<tr><td>Data Source</td><td>Time consumption in the authentication phase.</td></tr>
<tr><td>Indicator</td><td>One of the most important factors is the users' opinion and the usability of the system.</td></tr>
<tr><td>Reliability</td><td>The time consumption during the authentication phase depends on how well the user understands the system and how it is implemented. Using >30 test persons will strengthen statistical reliability of the results.</td></tr>
<tr><td>Validity</td><td>The validity of this metric is good.</td></tr>
</table>

Table 12: Metric for measuring speed of performance

3.5.3 Rate of errors by users

If the system has too many errors by users, something might be wrong with the authentication system or the implementation of it. Employees most likely forget their passwords four times a year on average [37]. The cost of resetting the passwords of thousands of employees is then astronomical. If using biometric authenticators, one might be affected by the fact that the biometric technology/device is difficult to use or have too high threshold values.

The metric measuring the rate of errors conducted by the users of the authentication system is shown in Table 13.

<table>
<tr><td>Metric ID</td><td>UM-3</td></tr>
<tr><td>Name</td><td>Rate of errors by users</td></tr>
<tr><td>Performance Goal</td><td>Measure the rate of errors performed by the users of the authentication system.</td></tr>
<tr><td>Performance Objective</td><td>Determine the rate of errors, both failure to enrol and failure to acquire, as well as other failures like e.g. when users forget their password or PIN.</td></tr>
<tr><td>Metric</td><td>Rate of errors by users.</td></tr>
<tr><td>Purpose</td><td>To measure the rate of errors by users. To many errors might indicate an error or configuration failure in the authentication system.</td></tr>
<tr><td>Implementation Evidence</td><td>How many errors are commited by the current user?
_____</td></tr>
<tr><td>Frequency</td><td>Once pr user/person.</td></tr>
<tr><td>Formula</td><td>Average rate of errors performed by the users.
<table>
<tr><td>Points</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td></tr>
<tr><td>Error in %</td><td><5</td><td>5-10</td><td>10-15</td><td>15-20</td><td>>20</td></tr>
</table></td></tr>
<tr><td>Data Source</td><td>Counting number of errors performed.</td></tr>
<tr><td>Indicator</td><td>One of many factors affecting the usability. Many errors may indicate configuration failures in the system or that the system might not be good enough.</td></tr>
<tr><td>Reliability</td><td>Using >30 test persons will strengthen statistical reliability of the results.</td></tr>
<tr><td>Validity</td><td>The validity of this metric is good.</td></tr>
</table>

Table 13: Metric for evaluation of rate of errors by users.

3.5.4 Rate of errors by the system

If an authentication system is to be put into practice and use, it is important that the number of errors caused by the system is small or zero. One has to implement the system and test in practice to measure the amount of system errors, and to see how it functions in the real world. Determining system errors is therefore a time consuming task, but still very important.

The metric measuring the rate of systemerrors is shown in Table 14.

<table>
<tr><td>Metric ID</td><td>UM-4</td></tr>
<tr><td>Name</td><td>Rate of errors by the system</td></tr>
<tr><td>Performance Goal</td><td>Measure the rate of errors performed by the authentication system.</td></tr>
<tr><td>Performance Objective</td><td>Determine the rate of errors, both failure to enrol and failure to acquire, caused by the system.</td></tr>
<tr><td>Metric</td><td>Rate of errors caused by the authentication system.</td></tr>
<tr><td>Purpose</td><td>To measure the rate of errors caused by the system. Too many errors might indicate an error or configuration failure in the authentication system.</td></tr>
<tr><td>Implementation Evidence</td><td>1.How many errors are caused by the system during the processing of current user's data?
_____
2.Type of error?What went wrong?
_____
_____
_____</td></tr>
<tr><td>Frequency</td><td>Register errors once pr user/person.</td></tr>
<tr><td>Formula</td><td>Average rate of errors caused by the system during processing current user's data.
<table>
<tr><td>Points</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td></tr>
<tr><td>Error in %</td><td>0</td><td>0-0.5</td><td>0.5-1.0</td><td>1.0-1.5</td><td>>1.5</td></tr>
</table></td></tr>
<tr><td>Data Source</td><td>Counting number of errors during the processing of current user's data.</td></tr>
<tr><td>Indicator</td><td>One of many factors affecting the usability. Many errors might indicate configuration failure(s) in the system or that the system might not be good enough.</td></tr>
<tr><td>Reliability</td><td>Using >30 test persons will strengthen statistical reliability of the results.</td></tr>
<tr><td>Validity</td><td>The validity of this metric is good.</td></tr>
</table>

Table 14: Metric for evaluation of system errors.

3.5.5 Subjective satisfaction

The most important information regarding the usability of the authentication system is the feedback from the user. The users' subjective opinions are valuable but somewhat difficult to measure. It is therefore important to use a predefined scale when asking the users about their opinion about the system.

The metric measuring the users opinions is shown in Table 15.

3.6 Normalization method

Score normalization refers to changing the location and scale parameters of the matching score distribution at the output of the individual matchers, so that the scores of different matchers are transformed into a common domain. Jain et al. [52] discuss score normalization in multimodal biometric systems. In a good normalization scheme, the estimates of the location and scale parameters must be robust and efficient. Robustness refers to the insensitivity to the presence of random errors (outliers). Efficiency refers to the proximity of the obtained estimate to the optimal estimate when the distribution of the data is known. [52] also refers to Snelick et al. [53] who evaluated the effects of normalization techniques like min-max, median, and fusion methods like sum of scores, min and max

Metric ID	UM-5.
Name	Subjective satisfaction
Performance Goal	Measure how the system affects the users and record the users opinion of the system.
Performance Objective	Determine whether or not the system affects the subjective satisfaction of the user and if the system bring up any privacy issues important for the user (important when using biometrics).
Metric	The users subjective satisfaction.
Purpose	To measure if the system affects the user or brings up any privacy issues.
Implementation Evidence	1.Are you satisfied with the use of the system?(0 is bad, 5 is excellent) 0[ ] 1[ ] 2[ ] 3[ ] 4[ ] 5[ ] 2.Do you belive the system will affect any privacy issues? Not at all[ ] Maybe[ ] Yes[ ] If yes or maybe: type of privacy issues: _____ _____ _____ 3.How will you evaluate the usability f the system?(0 is useless, 5 is excellent) 0[ ] 1[ ] 2[ ] 3[ ] 4[ ] 5[ ]
Frequency	Once pr user/person.
Formula	Average score given by the users. Score is given by the ranking places given by these average scores. Score or ranking from 1-6.
Data Source	The score given by the users.
Indicator	The users subjective satisfaction of the system is the most important information regarding the usability.
Reliability	The reliability of the test depends on how serious the users evaluate it, and the knowledge of the users. Using >30 test persons will strengthen statistical reliability of the results.
Validity	The validity of this metric is very good.

Table 15: Metric for evaluation of subjective satisfaction of the system.

rule and sum rule. Their experiments showed that the min-max normalization followed by the sum of scores fusion method outperforms other schemes.

The simplest normalization technique is the min-max normalization, and is best suited for the case where the bounds(maximum and minimum values) of the scores produced by a matcher are known. In this case, we can easily shift the minimum and maximum scores to 0 and 1, respectively. Given a set of matching scores s_k, k = 1,2,....,n, the normalized scores are given by

$$s'_k = \frac{s_k - min}{max - min} \tag{3.1}$$

Min-max normalization retains the original distribution of scores except for a scaling factor and transforms all the scores into a common range [0,1].

[52] concludes that if the location and scale parameters of matchings scores(minimum and maximum) of the individual modalities are known in advance, then simple normalization techniques like min-max would suffice.

When combining different authentication methods, integration of information may

take place prior to the verification/identification. Various levels of fusion are possible: fusion at the sensor level, feature extraction level, matching score level or decision level. Feature level fusion refers to combining different feature vectors from the different authentication methods in the system. When the feature vectors are non-homogeneous, e.g. they are obtained from different authentication methods, it is possible to concatenate them to form a single feature vector making it possible to compare the different authentication systems.

3.6.1 Euclidean distance

After normalizing the score, Euclidean distance is used to calculate the best authentication system according to the metrics. Even though the metrics take discrete value, see Chapter 3.3 and 3.5, the distance may be a continous value. The distance function *d*, is given by the following expression:

$$d = \sqrt{\sum_{i=1}^{n} | x_i - y_i |^2} \tag{3.2}$$

4 Experimental work

The user test or questionary was designed to determine how usable the different authentication systems are and how the participants evaluate usability and perceived security. It was of particular interest to determine which one of usability and security influences their choices the most.

4.1 Use of personal data

Due to the fact that fingerprints are viewed as personal data, it turned out that NSD[1] had to be applied. It was done in a form of a statement about using fingerprint authentication in the experiment.

4.2 Type of evaluation

The Best Practices in Testing and Reporting Performance of Biometric Devices [54] is a guideline widely accepted for testing biometric devices. There are three basic types of evaluation of biometric systems:

1. Technology evaluation: The goal of technology evaluation is to compare competing algorithms from a single technology.
2. Scenario evaluation: The goal of scenario testing is to determine the overall system performance in a prototype or simulated application.
3. Operational evaluation: The goal of operational testing is to determine the performance of a complete biometric system in a specific application environment with a specific target population.

The evaluation of the different authentication methods performed in this thesis is to be considered as an operational evaluation.

4.3 Pilot test

The first version of the questionary was formed using the usability metrics in Section 3.5. To make the questionary as usable and appropriate as possible, a pilot test was run in order to detect errors and modify the test. Ten participants conducted the pilot test and made some useful and critical comments. The participants in the pilot test were selected with regard to different skills, experiences and motivations.

One significant issue brought to day by this pilot test, was that people with little or no significant experience in the use of computers, failed to answer the questionary form. Due to this it was concluded that the test was to be run in an environment where the users possessed technological experience, thus making the type of evaluation operational. HiG was then chosen to be the most appropriate alternative arena for conducting the experiment.

[1] NSD, Norsk Samfunnsvitenskapelig Datatjeneste AS

4.4 Experimental design

4.4.1 Software and hardware

An application that enables selecting and combining different authentication methods has been developed [55]. The methods implemented are username, password, smart card with PIN and fingerprint.

The screen shots from the SmartFinger application are available in Appendix B. The main application window for the administrator of the experiment is shown in Fig. 2.

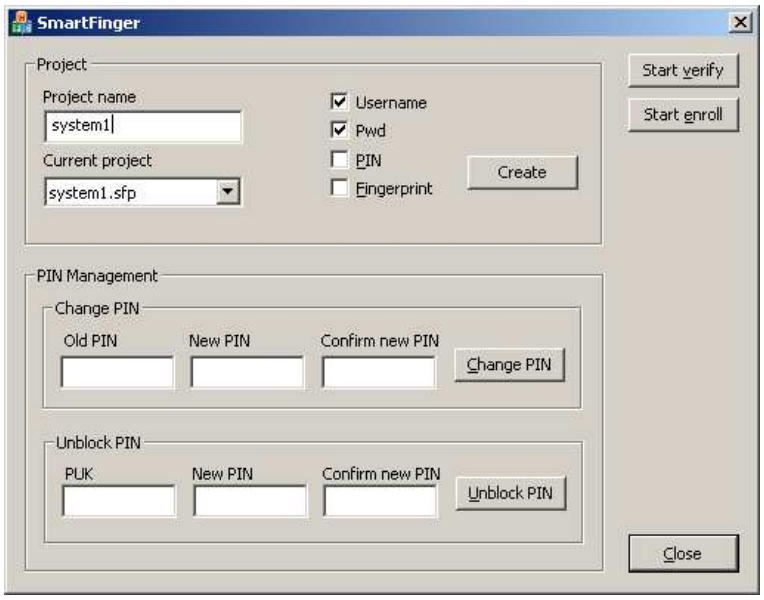

Figure 2: SmartFinger application

Smart card and smart card reader

The smart card used was a Multos Developer card [56], 48k Infineon, delivered by Buypass AS [57], referred to as Buypass smart card. The smart card reader is a Cardman 2020 from Omnikey Corp [58], a common USB smart card reader.

Fingerprint reader

The fingerprint reader used in the experiment was a U are U 4000 Sensor delivered by DigitalPersona [59].

The user simply places his/her finger on the glowing sensor window, and the device quickly and automatically captures the fingerprint image. Onboard electronics calibrate the device and encrypt the image data before sending it over the USB interface. The product utilizes optical fingerprint scanning technology for superior image quality and product reliability.

4.4.2 Participants

The user test was run with 61 participants, all of whom were experienced users of computer with different skills and experience regarding authentication methods. All participants were chosen from the HiG- environment, both students and employees. They represented a mix of ages, genders, educational levels and areas of professional expertise.

Figure 3: Multos 48k Infineon Developer card.

Figure 4: Omnikey Cardman 2020 smart card reader.

Figure 5: U are U 4000 Sensor from digitalPersona Inc.

The participants had to have some technical skills and computer experience, described in more details in Chapter 4.3, to be able to answer the questionary, see Appendix A.

The number of participants was obviously sufficient to determine effects and differences. [54] provides no statistical method for determining the required size of the test, but the number should be as large as practicable. 30 is the general number of participants, but one has to keep in mind that there are several important factors that may influence the decision about this number [60].

4.4.3 Test systems

The different methods made available in our test application are username, password, smartcard with 4 digit PIN and fingerprint. This led to the opportunity of testing $4!=24$ different combinations.

The fact that a smart card is a personalized token rules out the combination of username together with smartcard. A system using all these methods together will lead to a secure authentication, but it will be time consuming and thus impracticable. This system can only be used in highly secured institutions, e.g. military, and it will probably be more cost effective to implement iris or retina scan instead of fingerprinting. Therefore this system is also ruled out, leading to the final list of systems presented in Table 16.

#	**Authentication methods**
1	Username and password
2	Smart card with PIN
3	Fingerprint
4	Password and smart card with PIN
5	Username, password and fingerprint
6	Fingerprint and smart card with PIN

Table 16: Test systems

4.4.4 Questionnaire

After running the pilot test, a new version of the questionnaire was written, see Appendix A. In order to define the final version of the questionnaire, [61] was used as a reference. The questionnaire is used to collect information on perceived security and usability.

The role of the questions was to introduce the users in order for them to be aware of what was important regarding security, usability and effort needed. The system with which the participants were not familiar was in this way introduced to them, in order to make them capable of ranking the systems at the end of the experiment.

4.5 Experimental procedure

The participants were selected one by one, and brought to a seperate room to conduct the experiment. In the prephase of the experiment, each participant was briefed on the test scenario and given the questionary containing the information needed and the questions to be answered.

4.5.1 Enrolment

The registration phase, called enrolment, is when the person saves input to the system, and if needed a biometric image is captured, in this case a fingerprint. During this step there are mainly two scenes, the registration and the verification of the newly registered template, which might lead to errors [54]:

- The "failure to enroll" rate is the proportion of the population for whom the system is unable to generate repeatable templates, referred to as FTE.
- The "failure to aquire" rate is the proportion of attempts for which the system is unable to capture or locate an image of sufficient quality.

The enrolment phase in this experiments additionaly needs the registration of a username and password, see Picture 7. The usernames are set to be the first two charaters in the first name followed by the first two characters in the participants surname, e.g. Roar Sollie gets the username *roso*. The password is set to be Smart2005, containing both upper case, lower case and numbers. After the username and password registration, the participants must enroll their fingerprint of optional finger to complete the enrolment phase.

4.5.2 Identification and verification

After the enrolment, system 1, username and password, were selected. Current participant was then introduced to the application, showing two buttons, "Start test" and "Cancel", see Picture 8 Appendix B. When logging on to a computer the user usually has to

press "Ctrl"+"Alt"+"Del"- button on the keyboard, for the log on screen to appear. In this application the "Start test"- button represents this procedure.

When pressing the "Start test"- button, log on screen for the selected system appears, see Appendix B for screen shots of the different systems.

In addition the "Start test"- button triggers a timer, which stops when current participant is successfully authenticated. The participants are not informed about this prior to the test, to avoid any stress moments or negligence regarding the results.

When the participant have been successfully authenticated, he/she answers the question regarding current authentication system. The next system to be tested is then selected, and the participant repeats the same procedure for all the authentication systems. When all systems were tested, the participant answers the summary questions, see Appendix A.

5 Security evaluation

In this chapter, a security evaluation of the different authentication systems tested depends on whether or not different security mechanisms are implemented. The different authentication methods are discussed and evaluated according to implemented security mechanisms. The scores of the evaluation of the different authencation systems according to the defined security metrics are shown in Table 17.

5.1 Username and password

Both username and password are in the "knows"- category, and are therefore easy to lend away and become a target of guessing and brute force attacks. The biggest problem of "good" passwords is that users forget them easily. Asking a user to recall a single user id and password for one system may seem reasonable, but with proliferation of passwords, users are increasingly unable to cope with [62]. To be secure, i.e. not to be guessable, a password must be a random combination of numbers, symbols and letters. Unfortunately, these types of passwords are more difficult for people to remember than e.g. names or associative words [13]. It is not possible to remember all well-generated, secure and different passwords on every system, and the consequence is that one has to write them down [63].

In addition to the structure of the password, important questions are the storage and encryption of the password. Passwords and PINs can be hacked, guessed or lent away, and secure tokens can be lost or lent away. In addition to these factors, one has the cost when a password needs to be reset or changed and the helpdesk or network administrator has to be contacted [37].

Username and password get no score on SM-1 and SM-2 due to the fact that they measure liveness testing and tamper resistance. In the evaluation of SM-3 it is supposed that the username and password are stored in a secure way and encrypted using RSA wiht 2048 bit key size, giving the score 4: 1 point because of the authentication and encryption and 3 points for the size of the RSA key. SM-4 refers to fall-back mode, usually traditional authentication, and is needed when biometric authentication methods are used. The score is therefore zero on this metric. Security metric nr.5 deals with multiple authentication. Username and password are two methods in the "*knows*" category, which results in two points.

5.2 Smart card with PIN

The smart card used is a Multos Developer card [56], 48k Infineon, delivered by Buypass AS [57]. The routines for key generation are sertified according to the highest ITSEC level and secondary highest common criteria level.

Smart card with PIN get no score on SM-1 because it measures liveness testing which refers to biometrics. The security regarding tamper resistance provides a maximum score of two on SM-2. The chip on the smart card used supports up to 2048 bits RSA encryption, and the application on the card, the Buypass Electronic ID supports 2032 bits RSA encryption. This gives the smart card with PIN a score of four points in SM-3. SM-4 refers

to fall-back mode, usually traditional authentication, and is needed when biometric authentication methods are used. The score is therefore zero on this metric. Smart card with PIN consists of both a token and a secret PIN, refering to two of the authentication categories, giving it a score of 4 points on SM-5.

5.3 Fingerprint

The fingerprint reader, U are U 4000 Sensor, delivered by DigitalPersona has onboard electronics which calibrates the device and encrypts the image data before sending it over the USB interface, according to the product description [59]. It is also said to reject latent fingerprints and counterfeit image rejection. The product description does not describe or say anything about the cryptographic algortihm used or size of encryption keys.

The fact that we managed to make an artificial fingerprint out of plaster and silicon, which was not detected by this fingerprint sensor [64], puts the possibility of counterfeiting image rejection under suspicion. A fingerprint sensor with liveness detection, e.g. blood circulation, heart beat or perspiration pores, should not be that easy to counterfeit.

The use of a biometric, in this case the fingerprint, requires a fall-back mode for use in cases of malfuntions or missing biometric feature. In the experiment and security evaluation, username and password are considered the fall-back mode when needed.

The fact that fingerprint is a biometric gives it one point in SM-1. The specification of the fingerprint sensor do not mention advanced tamper resistance in the key specification or features. The fact that it is a token and that data is encrypted before transferred over the USB interface, makes the tamper resistance moderate, and it gets one point according to SM-2. The product description of the fingerprint sensor states that the image data is encrypted before the image is transferred over the USB interface. The fingerprint sensor gets two points in SM-3, because the communication is authenticated and encrypted, and the fact that it uses a proprietary algorithm. As stated earlier, username and password are used as fall-back mode, giving fingerprint one point regarding SM-4. Fingerprint is only one authentication method from one of the categories, giving it a score of 1 points on SM-5.

5.4 Password and smart card with PIN

Neither password nor smart card with PIN are a biometric, making the score of SM-1 and SM-4 zero. The smart card offers the advanced tamper resistance giving two points on the tamper resistance metric. The fact that both password and the smartcard offers high encryption results in four points regarding SM-3. Password and smartcard with PIN consists of two methods in the "*knows*" category and one from the "*has*" category, making the score from SM-5 five points.

5.5 Username, password and fingerprint

Fingerprint offers the biometric authentication method resulting in one point on SM-1, and the fingerprint sensor gives an additional point on the tamper resitance metric. Username and password is encrypted giving it four points on the SM-4. Username, password and fingerprint results in a score of five points on the multiple authentication metric.

5.6 Fingerprint and smart card with PIN

Fingerprint is the biometric giving one point on the liveness and the traditional authentication metric. The smart card offers advanced tamper resistance, resulting in two points on SM-2. The smart card offers high encryption and four points on the secure communication metric. Fingerprint and smart card with PIN results in a total of seven points on SM-5.

5.7 Security ranking of the systems

The systems tested in the experiment are ranked in Table 16 according to security. Precautions regarding different authentication methods are mentioned previously in this chapter.

Table 17 shows the resulting scores of the different authentication systems tested according to the metrics. The maximum possible score according to each metric is also listed. The scores are normalized and Euclidean distances are calculated, see Chapter 3.6.

System	**SM-1**	**SM-2**	**SM-3**	**SM-4**	**SM-5**	**d-value**
Username and password	0	0	4	0	2	1.898
Smart card with PIN	0	2	4	0	4	1.513
Fingerprint	1	1	2	1	1	1.544
Password and smart card with PIN	0	2	4	0	5	1.477
Username, password and fingerprint	1	1	4	1	5	1.167
Fingerprint and smart card with PIN	1	2	4	1	7	0.972
Maximum score on the metrics	4	2	5	3	8	

Table 17: Security score table.

The ranking of the systems according to the calculated Euclidean distances is:

1. Fingerprint and smart card with PIN (system 6)
2. Username, password and fingerprint (system 5)
3. Password and smart card with PIN (system 4)
4. Smart card with PIN (system 2)
5. Fingerprint (system 3)
6. Username and password (system 1)

6 Results

In this chapter, we present the results and answers from the participants in the experiment. One of the participants chose not to answer question 15 due to the lack of knowledge and experience in computer security and authentication methods. Results from this person are therefore missing in the ranking of the different authentication methods.

6.1 Username and password

As many as 40 of the participants meant that the username and password had no or little effort, and nobody thought that it was much effort. When it comes to the security for use in an industrial context, as much as 50.8% answered that the security was excellent, but for home use the answeres were evenly spread. Over 80% of the participants believed that username and password was more than usable enough for use at home and in an industrial context.

When the participants ranked the systems, 68.3% of the participants ranked username and password as the poorest authentication system regarding security, but as much as 30% ranked the system second and 35% third when it came to the usability.

6.2 Smart card with PIN

75.4% or 46 participants meant that smartcard with four digit PIN, had little or no effort. When it came to security, both for home use and in an industrial context, approximately 50% of the participants found this system excellent. Smartcard with PIN also scored high on the usablity issue with over 50% giving it top grade, both for use at home and work.

Regarding the ranking of the different systems, smartcard with PIN, ended up with 58.3% ranking them fifth of the six authentication methods tested. Despite this, 50% of the participants ranked it second regarding usability.

6.3 Fingerprint

Two of the participants had to chose another finger than the first finger they tried to enroll, due to the fact that their preferred finger was of poor quality. Fingerprint scored highest on the question of effort with as much as 96.7%, or 59 out of 61 participants, answering that it hat no or little effort. 60.7% and 55.7% meant that the security was excellent according to home use and for use in an industrial context respectively. When it comes to the question of usability, as many as 48 of 61, or 78.7%, of the participants gave it the highest score.

The summary question with ranking of the system shows that fingerprint is number one when it comes to the question of ease of use, with a total of 81.7% ranking it number one. Regarding the security fingerprint, as a single authentication method, ended up third with 40% of the votes.

6.4 Password and smart card with PIN

Regarding password and smart card with PIN, results show that the test persons think that it requires more effort than the previous systems tested. This system scores high

when it comes to the question of security, both for home use and at work, with over 50% of the participants giving it top score. When it comes to the question of usability, the results are more scattered but still showing that over 50% gave the system score four or five out of maximum five.

In the ranking of the systems, password and smart card with PIN ended up with 50% of the participants ranking it fourth according to security, and as much as 38.3% ranked it the last when it came to the usability.

6.5 Username, password and fingerprint

Over 70% of the participants thought that username, password and fingerprint required some effort, but when it came to the issue of security, this system scored high. As much as 67.2% graded its security excellent for use in an industrial context, and 59% for home use. Even though the usability results were more evenly scattered, over 65% gave it score four or five out of maximum five points.

The combination of username, password and fingerprint was ranked second with 34 of 60 votes, on the ranking of security, but ended up the last when it came to the usability, with 41.7% of the votes.

6.6 Fingerprint and smart card with PIN

24 of the 61 participants thought that fingerprint and smart card with PIN required little or no effort. Over 80% gave it score one or two, where one indicates little or no effort and five indicates that the system required much effort. This system scored high regarding security, with 70.5% and 62.3% according to use at work and home use respectively. Fingerprint and smart card with PIN also scored high according to the usability, with over 75% giving it score four or five.

The combination of fingerprint and smart card with PIN was ranked highest regarding the security, with 68.3% of the votes, but ended up fifth of six, regarding the ease of use.

6.7 Summary of results

Summing perceived usability and security from the ranking performed by the participants, the total "winner" seems to be the fingerprint as a single authentication method, see Table 18. Most of the participants mentioned the ease of use regarding the fingerprint, even though only nine of the 61 participants had experience using fingerprint authentication. The authentication methods containing the fingerprint, ended up on the three first places regarding perceived security and the two best places regarding perceived usability. The main purpose of the experiment was to have an evaluation of usability of the systems. The system ranked highest according to usability were therefore ranked highest when the total scores were equal. System number four, password and smart card with PIN, and system number one, username and password, got the same total score. This is the reason why system number one is ranked better than system number four.

The ranking of the systems when summing perceived usability and security is then as follows (total score in parentheses):

1. Fingerprint(4)
2. Fingerprint and smart card with PIN(5)
3. Smart card with PIN(7)

4. Username, password and fingerprint(8)
5. Username and password(9)
6. Password and smart card with PIN(9)

Balancedness, the difference between perceived usability and security, is to see whether or not the authentication method has a good balance of the two factors, see Table 18. This is an alternative way to the summarization ranking of the systems. When the difference of the systems are equal, the usability ranking decides which one is ranked best.

The ranking of the systems when looking at the balance between perceived usabilty and security:

1. Password and smart card with PIN(1)
2. Fingerprint(2)
3. Smart card with PIN(3)
4. Username and password(3)
5. Fingerprint and smart card with PIN(3)
6. Username, password and fingerprint(4)

	Authentication system					
	1	2	3	4	5	6
Number of users with experience (total 61).	61	33	9	10	4	3
Average time used (in seconds)	13.3	10.6	6.2	23.5	17.7	14.8
Number of errors	7	7	7	9	4	5
Ranking according to perceived security.	6	5	3	4	2	1
Ranking according to perceived usability.	3	2	1	5	6	4
Total ranking score (security + usability)	9	7	4	9	8	5
Balancedness (difference between usability and security)	3	3	2	1	4	3

Table 18: Summary of average time, number of errors; the ranking of the systems is based on the answers to the question 15 as well as to the question if users have experience using this method or not.

When evaluating the results from the participants according to the usability metrics defined in Section 3.5 and calculating the Euclidean distance, see Table 19, the ranking of the systems was the same as the ranking performed by the participants, see Table 18.

6.8 Discussion and analysis

The results regarding username and password are most likely coloured by the fact that this is the method most used, making the participants familiar with this system. Question 16 in the questionnaire shows that all the participants have experience with username and password, and this is also the method used to log on to the computers at HiG.

Little knowledge regarding the security regarding the use of smart card and smart card technology might have influenced the results. A smart card offers a level of tamper resistance since the chip is embedded and sensitive data can be encrypted. The combination of biometrics with smart cards and PKI seems to be a secure and highly usable

System	**UM-1**	**UM-2**	**UM-3**	**UM-4**	**UM-5**	**d-value**
Username and password	5	4	3	5	4	3
Smart card with PIN	5	4	3	5	5	$\sqrt{6}$
Fingerprint	5	5	4	5	6	2
Password and smart card with PIN	4	2	3	5	2	$\sqrt{30}$
Username, password and fingerprint	4	3	4	5	1	$\sqrt{31}$
Fingerprint and smart card with PIN	4	4	4	5	3	$\sqrt{12}$
Maximum score on the metrics	5	5	5	5	6	

Table 19: Perceived usability score table.

system and also has the possibility of being used over the Internet.

Fingerprint has the ease of use and the fact that it is a biometric, a part of the person, makes the perceived security and usability high. If fingerprint readers are integrated on personal computers and laptops or embedded in a smart card [29, 30, 35, 37], this makes the ease of use further improved.

One important question in this thesis is the relation between perceived security obtained by the experiment and the author's security evaluation of the authentication systems. In Table 20, each system is ranked, 1 is the best and 6 is the lowest ranked system .

System	Perceived usability	Perceived Security	The author's security evaluation
Username and password	2	6	6
Smart card with PIN	3	4	4
Fingerprint	1	5	5
Password and smart card with PIN	5	2	3
Username, password and fingerprint	6	3	2
Fingerprint and smart card with PIN	4	1	1

Table 20: Comparison of perceived security in the experiment and the author's security evaluation.

The ranking is based on a comparison of the perceived usability and the author's security evaluation of the systems based on the security metrics, Section 3.3. This is because the participants' level of knowledge and experience regardning computer security and authentication mechanisms are unknown.

System	Sum	Balancedness
Username and password	8	4
Smart card with PIN	7	1
Fingerprint	6	4
Password and smart card with PIN	8	2
Username, password and fingerprint	8	4
Fingerprint and smart card with PIN	5	3

Table 21: Ranking of the systems according to sum and balancedness.

As for the sum and balancedness of the systems, three of the systems ended up with equal scores in both cases. Due to the fact that the author's belief is that security should be weighted more than usability, this is what separated them according to the rankings.

Ranking regarding the sum of perceived usability and evaluated security:

1. Fingerprint and smart card with PIN
2. Fingerprint
3. Smart card with PIN
4. Username, password and fingerprint
5. Password and smart card with PIN
6. Username and password

Ranking regarding the balancedness between perceived usability and evaluated security:

1. Smart card with PIN
2. Password and smart card with PIN
3. Fingerprint and smart card with PIN
4. Fingerprint
5. Username, password and fingerprint
6. Username and password

7 Conclusion

There is an increasing focus on computer security in todays modern society. One important problem regarding computer security is the use of authentication methods when logging on to computers. Many companies and institutions are focusing on the structure and security of the passwords they use. Several publications describe how secure passwords are constructed and used. A known problem regarding use of secure passwords is how one ought to remember them all. Different and secure passwords in every system a person uses, will lead to the need of writing them down.

This project was supposed to give an indication of security and usability regarding different authentication methods. An experiment, with participants and questionaire, was conducted to give an indication on the level of perceived security and usability. The participants were selected within the HiG- environment, both students and employees, having in mind that they have technical skills. In the process of making this questionaire, five security metrics and five usability metrics were defined. These metrics were supposed to cover the main questions regarding security and usability in an authentication process.

The experiment shows that the use of biometric authentication methods are accepted among the participants. The ranking of the tested systems shows that they believed fingerprint authentication was secure and usable. The top three ranked systems regarding perceived security contained the fingerprint, and the best ranked system regarding usability was the fingerprint as a single authentication method. The results also show that smart card with PIN has the best balancedness regarding usability and security. It is therefor reasonable to implement a combination of different authentication methods.

The set of metrics, and results and analysis from the questionaire will hopefully inspire others in further work and similar projects.

8 Further work

The metrics proposed in this thesis are supposed to be a useful tool when evaluating authentication methods according to usability and security. To see if the metrics are useful, they should be implemented, tested and used in a real life context, to measure the users' opinion and retention over time. Usability testing of biometrics other than fingerprint, to see how people experience them, is an important question needed to be further explored. Other authentication methods from the different categories, "*has*" and "*knows*", also need further testing. Other hardware tokens, passfaces and passphraces are some methods needed to be further tested.

Little research has been done within the cost/benefit analysis of different authentication methods, especially biometrics. Cost, benefit and effort when implementing different systems seem to bee necessary to analyze. The cost of smart cards and biometric tokens has become cheaper to be useful and suitable for use at home as well as in an industrial context.

Bibliography

[1] John W. Creswell. *Research Design; Qualitative, Quantitative and Mixed Methods Approaches*. Sage Publications, second edition edition, 2003.

[2] Neil J. Salkind. *Exploring Research*. Prentice Hall, 5th edition, 2002.

[3] Marilyn Chun. Authentication mechanisms, which is best?, 2001. http://www.giac.org/practical/gsec/Marilyn_Chun_GSEC.pdf.

[4] John Abbott. Smart cards: How secure are they? *GSEC Practical v1.3*, 2002. http://www.sans.org/rr/papers/index.php?id=131.

[5] Bruce Schneier and Adam Shostack. Breaking up is hard to do: Modeling security threats for smart cards, 1999. http://www.schneier.com/paper-smart-card-threats.html.

[6] David D. Zhang, editor. *Biometric Solutions For Authentication in an E-World*. The Kluwer International Series in Engineering and Computer Science. Kluwer Academic Publishers, 2002.

[7] Marijana Kosmerlj. Passport of the future - biometrics against identity theft. Master's thesis, Royal Institute of Technology, Sweden, 2004.

[8] Gregory Williams. More than a pretty face: Biometrics and smartcard tokens. *GSEC*, 2002. http://www.sans.org/rr/papers/6/125.pdf.

[9] G. R. Ganger. Authentication confidences. http://citeseer.ist.psu.edu/456656.html, 2001. Technical Report CMU-CS-01-123.

[10] NIST. Fips 190, guideline for the use of advanced authentication technology alternatives, 1994. http://www.itl.nist.gov/fipspubs/fip190.htm.

[11] L. Bechelli, S. Bistarelli, and A. Vaccarelli. Biometrics authentication with smartcard, 2002. http://citeseer.ist.psu.edu/bechelli02biometrics.html.

[12] N. Poh, S. Bengio, and J. Korczak. A multi-sample multi-source model for biometric authentication, 2002. http://citeseer.ist.psu.edu/thian02multisample.html.

[13] S.Brostoff and A.Sasse. Are passfaces more usable than passwords? A field trial investigation., 2000. http://oneman.cs.ucl.ac.uk/brostoff_sasse.pdf.

[14] Vaclav Matyas and Zdenek Riha. Biometric authentication- security and usability. http://www.fi.muni.cz/usr/matyas/ cms_matyas_riha_biometrics.pdf, 2002. Faculty of Informatics, Masaryk university Brno, Czech Republic.

[15] M. Dacier, Y. Deswarte, and M. Kaaniche. Quantitative assessment of operational security: Models and tools. citeseer.ist.psu.edu/dacier96quantitative.html, 1996.

[16] Timothy J. Hazen, Eugene Weinstein, and Alex Park. Towards robust person recognition on handheld devices using face and speaker identification technologies. In *Proceedings of the 5th international conference on Multimodal interfaces*, pages 289–292. ACM Press, 2003. http://doi.acm.org/10.1145/958432.958485.

[17] Niall A. Fox, Ralph Gross, Philip de Chazal, Jeffery F. Cohn, and Richard B. Reilly. Person identification using automatic integration of speech, lip, and face experts. In *Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications*, pages 25–32. ACM Press, 2003.

[18] R. Dhamija. Hash visualization in user authentication, 2000. http://citeseer.ist.psu.edu/dhamija00hash.html.

[19] Rachna Dhamija and Adrian Perrig. Deja vu: A user study using images for authentication. In *Proceedings of the 9th USENIX Security Symposium*, 2000. http://citeseer.ist.psu.edu/326534.html.

[20] Lawrence O'Gorman. Comparing passwords, tokens, and biometrics for user authentication, 2003. http://www.research.avayalabs.com/user/logorman/compareAuthent.pdf.

[21] Chiara Braghi. Biometric authentication. http://citeseer.ist.psu.edu/436492.html.

[22] Richard E. Smith. *Authentication: From Passwords to Public Keys*. Addison-Wesley Pub Co, 2001.

[23] Ruud Bolle Anil Jain and Sharath Pankanti, editors. *Biometric, Personal Identification in Networked Society*. The Kluwer International Series in Engineering and Computer Science. Kluwer Academic Publishers, 1998.

[24] Dirk Scheuermann Ulrich Waldmann and Claudia Eckert. Protected transmission of biometric user authentication data for oncard-matching. http://www.sit.fhg.de/ZAVIR/WSE04.pdf, 2004.

[25] Itsec, information technology security evaluation criteria. http://www.cesg.gov.uk/site/iacs/itsec/media/formal-docs/Itsec.pdf, 1991.

[26] Bruno Struif. Use of biometrics for user verification in electronic signature smartcards. http://www.sit.fhg.de/ZAVIR/str01.pdf, 2001.

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

[28] A. Jain L. Hong and S. Pankanti. Biometric identification. pages 91–98. Communications of the ACM (CACM), 2000. http://biometrics.cse.msu.edu/publications.html#multi.

[29] Stefano Bistarelli Giampaolo Bella and Fabio Martinelli. Biometrics to enchance smartcard security. http://www.sci.unich.it/\~bista/papers/papers-download/mocviatocfinal.p%df, 2003.

[30] Negar Kiyavash T. Charles Clancy and Dennis J. Lin. Secure smartcard-based fingerprint authentication. http://portal.acm.org/ft_gateway.cfm\%3Fid\%3D982516\%26type\%3Dpdf\%26%dl\%3DACM\%26dl\%3DACM\%26CFID\%3D11111111\%26CFTOKEN\%3D2222222, 2003.

[31] Patrick G. McLean. A secure pervasive environment. In *Proceedings of the Australasian information security workshop conference on ACSW frontiers 2003*, pages 67–75. Australian Computer Society, Inc., 2003.

[32] Stephen T. Kent and Lynette I. Millett. *Who Goes There?: Authentication Through the Lens of Privacy*. CSTB Publications, 2003.

[33] Andrew S. Patrick. Usability and acceptability of biometric security systems. *Lecture Notes in Computer Science*, 3110 / 2004, 2004.

[34] Robert Stocker. Applying usability testing and techniques to develop user-centered security. http://eies.njit.edu/~turoff/coursenotes/CIS732/samplepro/testing_and_s%ecurity.htm, 2000.

[35] Tricia Olsson. Strenghtening authentication with biometric technology. *GSEC Practical 1.4b*, 2003. http://cnscenter.future.co.kr/resource/security/authen/1226.pdf.

[36] Applied Computer Security Associates. Workshop on information security system scoring and ranking, 2001. http://www.acsac.org/measurement/proceedings/wisssr1-proceedings.pdf.

[37] William J. Lawson. Too many passwords... http://www.icdri.org/biometrics/Too\%20Many\%20Passwords.htm, 2002.

[38] NIST. Nist 800-55, security metrics guide for information technology systems. *NIST paper*, July 2003.

[39] Johnny Mathisen. Measuring information security awareness. Master's thesis, Royal Institute of Technology, Sweden, 2004.

[40] Edward G. Carmines and Richard A. Zeller. *Reliability and Validity Assessment*. Sage University Paper, 1979.

[41] Andrew Odlyzko. Economics, psychology and sociology of security. http://www.dtc.umn.edu/~odlyzko/doc/econ.psych.security.pdf, 2003.

[42] Marie Sandström. Liveness detection in fingerprint recognition systems. Master's thesis, Linköpings Tekniska Högskola, Sweden, 2004.

[43] Geir Olav Dyrkolbotn. *Smart Cards - Robustness against Electromagnetic Side-Channel Attacks*. PhD thesis, Gjøvik University College, 2005.

[44] Prof. Jean-Jacques Quisquater. Side channel attacks, state-of-the-art. 2002.

[45] Thomas S. Messerges, Ezzat A. Dabbish, and Robert H. Sloan. Examining smart-card security under the threat of power analysis attacks. *IEEE Trans. Comput.*, 51(5):541–552, 2002.

[46] Paul Kocher, Joshua Jaffe, and Benjamin Jun. Introduction to differential power analysis and related attacks. *Lecture Notes in Computer Science*, 1998.

[47] Paul Kocher, Joshua Jaffe, and Benjamin Jun. Differential power analysis. *Lecture Notes in Computer Science*, 1999.

[48] Arjen K. Lenstra and Eric R. Verheul. Selecting cryptographic key sizes. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 14(4):255–293, 2001.

[49] Common criteria for information technology security evaluation. `http://www.radium.ncsc.mil/tpep/library/ccitse/ccitse.html`, 1999.

[50] Bdpp, biometric device protection profile. `http://www.cesg.gov.uk/site/iacs/index.cfm?menuSelected=1\&displayPage=%19`, 2001. Draft Issue 0.82.

[51] Anil K. Jain, Arun Ross, and Salil Prabhakar. An introduction to biometric recognition. *IEEE Trans. Circuits Syst. Video Techn.*, 14(1):4–20, 2004.

[52] Anil K. Jain, Karthik Nandakumar, and Arun Ross. Score normalization in multimodal biometric systems. Technical Report MSU-CSE-04-14, Department of Computer Science, Michigan State University, April 2004.

[53] *Proceedings of the 5th International Conference on Multimodal Interfaces, ICMI 2003, Vancouver*. ACM, 2003.

[54] Best practices in testing and reporting performance of biometric devices. http://www.cesg.gov.uk/site/iacs/index.cfm?menuSelected=1&displayPage=19, 2000.

[55] Morten Johansen. `http://www.buypass.no`. Program developer.

[56] The Consortium Company MAOSCO Ltd. `http://www.multos.com/n`. Application Developer Cards for developing MULTOS Applications.

[57] Buypass AS. `http://www.buypass.no`. Securing Transactions.

[58] Omnikey Inc. `http://www.omnikey.com`. Smart Card Reader Technology.

[59] digitalPersona Inc. `http://www.digitalpersona.com`. U are U 4000 Sensor.

[60] Neil J. Salkind. *Exploring Research*. Prentice Hall, 5th edition, 2002.

[61] Frode Volden. `http://www.hig.no`. Personal communication.

[62] M. A. Sasse, S. Brostoff, and D. Weirich. Transforming the weakest link- a human/computer interaction approach to usable and effective security. *BT Technology Journal*, 19(3):122–131, 2001.

[63] J. Jeff, Y. Alan, B. Ross, and A. Alasdair. The memorability and security of passwords – some empirical results. citeseer.ist.psu.edu/yan00memorability.html, 2000.

[64] Tom Fladsrud and Roar S. Sollie. Circumvention of fingerprint scanners. http://www.roarsollie.net/skole/Circumvention\%20of\%20fingerprint\%20s%canners\%20-\%20Autentisering.pdf, 2004. IMT-5071 Authentication.

A Questionnaire

Registration information

Sex: ☐ Male ☐ Female

Username: _____(the two first letters in first name, and two first letters in surname, e.g. username for Roar Sollie is roso)

Password: **Smart2005**

PIN code for smart card: **3257**

System 1 - Username and password

1. Logon

   a. Was the logon successful?
   ☐ Yes ☐ No

   b. Did you find the logon procedure easy?
   Little effort ☐1 ☐2 ☐3 ☐4 ☐5 Too much effort

2. Conclusions

   a. Do you think it is possible to use similar logon system in an intranet or industrial context?

      i. Regarding security:
      No ☐1 ☐2 ☐3 ☐4 ☐5 Yes

      ii. Regarding usability:
      No ☐1 ☐2 ☐3 ☐4 ☐5 Yes

   b. Do you think this logon system can be implemented for home use, e.g. for use in online gambling or banking, or similar services including sensitive information or money transactions?

      i. Regarding security:
      No ☐1 ☐2 ☐3 ☐4 ☐5 Yes

      ii. Regarding usability:
      No ☐1 ☐2 ☐3 ☐4 ☐5 Yes

System 2 - Smart card with 4 digit PIN

3. Logon

   a. Was the logon successful?
   ☐ Yes ☐ No

   b. Did you find the logon procedure easy?
   Little effort ☐1 ☐2 ☐3 ☐4 ☐5 Too much effort

4. Conclusions

   a. Do you think it is possible to use similar logon system in an intranet or industrial context?

      i. Regarding security:
      No ☐1 ☐2 ☐3 ☐4 ☐5 Yes

      ii. Regarding usability:
      No ☐1 ☐2 ☐3 ☐4 ☐5 Yes

   b. Do you think this logon system can be implemented for home use, e.g. for use in online gambling or banking, or similar services including sensitive information or money transactions?

      i. Regarding security:
      No ☐1 ☐2 ☐3 ☐4 ☐5 Yes

      ii. Regarding usability:
      No ☐1 ☐2 ☐3 ☐4 ☐5 Yes

System 3 - Fingerprint

5. Logon

   a. Was the logon successful?
   ☐ Yes ☐ No

   b. Did you find the logon procedure easy?
   Little effort ☐1 ☐2 ☐3 ☐4 ☐5 Too much effort

6. Conclusions

   a. Do you think it is possible to use similar logon system in an intranet or industrial context?

      i. Regarding security:
      No ☐1 ☐2 ☐3 ☐4 ☐5 Yes

      ii. Regarding usability:
      No ☐1 ☐2 ☐3 ☐4 ☐5 Yes

   b. Do you think this logon system can be implemented for home use, e.g. for use in online gambling or banking, or similar services including sensitive information or money transactions?

      i. Regarding security:
      No ☐1 ☐2 ☐3 ☐4 ☐5 Yes

      ii. Regarding usability:
      No ☐1 ☐2 ☐3 ☐4 ☐5 Yes

7. Subjective satisfaction

   a. What is your personal opinion regarding the use of biometrics in a logon procedure, e.g. fingerprint, voice recognition?
   Useless ☐1 ☐2 ☐3 ☐4 ☐5 Excellent

System 4 - Password and smart card with 4 digit PIN

8. Logon

   a. Was the logon successful?
   ☐ Yes ☐ No

   b. Did you find the logon procedure easy?
   Little effort ☐1 ☐2 ☐3 ☐4 ☐5 Too much effort

9. Conclusions

   a. Do you think it is possible to use similar logon system in an intranet or industrial context?

      i. Regarding security:
      No ☐1 ☐2 ☐3 ☐4 ☐5 Yes

      ii. Regarding usability:
      No ☐1 ☐2 ☐3 ☐4 ☐5 Yes

   b. Do you think this logon system can be implemented for home use, e.g. for use in online gambling or banking, or similar services including sensitive information or money transactions?

      i. Regarding security:
      No ☐1 ☐2 ☐3 ☐4 ☐5 Yes

      ii. Regarding usability:
      No ☐1 ☐2 ☐3 ☐4 ☐5 Yes

System 5 - username, password and fingerprint

10. Logon

    a. Was the logon successful?
    ☐ Yes ☐ No

    b. Did you find the logon procedure easy?
    Little effort ☐1 ☐2 ☐3 ☐4 ☐5 Too much effort

11. Conclusions

    a. Do you think it is possible to use similar logon system in an intranet or industrial context?

        i. Regarding security:
        No ☐1 ☐2 ☐3 ☐4 ☐5 Yes

        ii. Regarding usability:
        No ☐1 ☐2 ☐3 ☐4 ☐5 Yes

    b. Do you think this logon system can be implemented for home use, e.g. for use in online gambling or banking, or similar services including sensitive information or money transactions?

        i. Regarding security:
        No ☐1 ☐2 ☐3 ☐4 ☐5 Yes

        ii. Regarding usability:
        No ☐1 ☐2 ☐3 ☐4 ☐5 Yes

System 6 - Smart card with 4 digit PIN and fingerprint

12. Logon

    a. Was the logon successful?
    ☐ Yes ☐ No

    b. Did you find the logon procedure easy?
    Little effort ☐1 ☐2 ☐3 ☐4 ☐5 Too much effort

13. Conclusions

    a. Do you think it is possible to use similar logon system in an intranet or industrial context?

        i. Regarding security:
        No ☐1 ☐2 ☐3 ☐4 ☐5 Yes

        ii. Regarding usability:
        No ☐1 ☐2 ☐3 ☐4 ☐5 Yes

    b. Do you think this logon system can be implemented for home use, e.g. for use in online gambling or banking, or similar services including sensitive information or money transactions?

        i. Regarding security:
        No ☐1 ☐2 ☐3 ☐4 ☐5 Yes

        ii. Regarding usability:
        No ☐1 ☐2 ☐3 ☐4 ☐5 Yes

14. Personal opinion

    a. What is your opinion if the fingerprint reader is integrated on the smart card, and the smart card reader is integrated on the computer?
    Worse ☐1 ☐2 ☐3 ☐4 ☐5 Better

15. Rank the systems tested, from 1 to 6, where 1 is the best. Rank with regard of security, usability, home use or for use at work.

System	Security	Usability	Home use	At work
Username and password				
Smart card with PIN				
Fingerprint				
Password and smart card with PIN				
Username, password and fingerprint				
Smart card with PIN and fingerprint				

16. Do you have any previous experience from similar systems? If yes, mark the corresponding cell in the matrix.

System	Work	Home use	No experience
Username and password			
Smart card with PIN			
Fingerprint			
Password and smart card with PIN			
Username, password and fingerprint			
Smart card with PIN and fingerprint			

B SmartFinger application

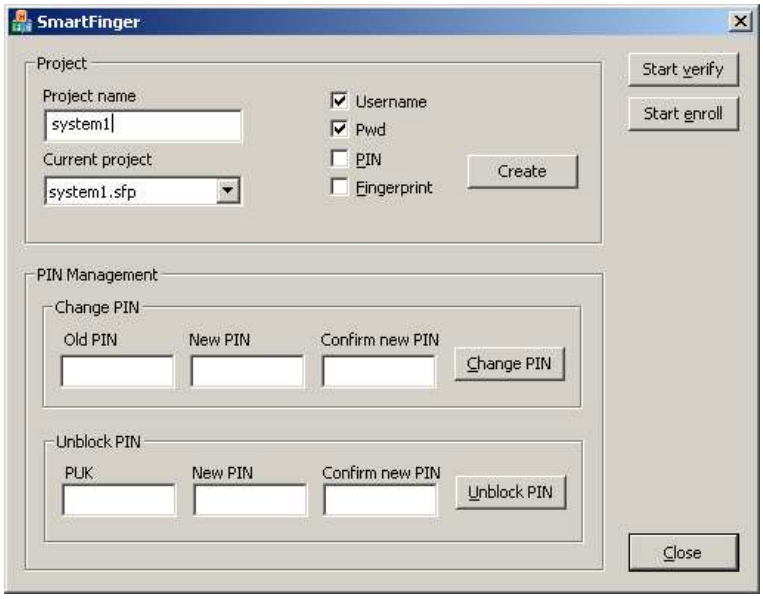

Figure 6: Main window of the application.

Figure 7: Registration of username, password and enrolment of the fingerprint.

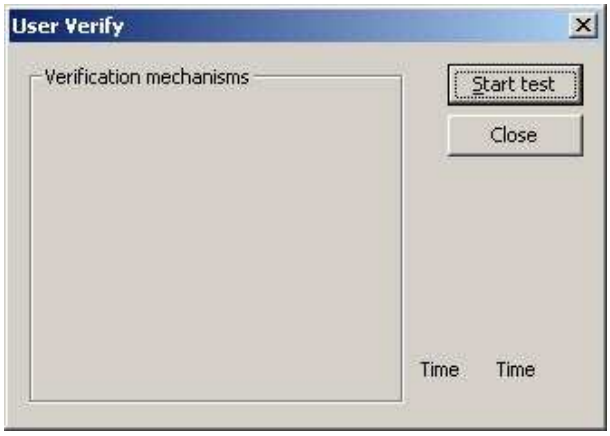

Figure 8: Press start to start the chosen authentication system.

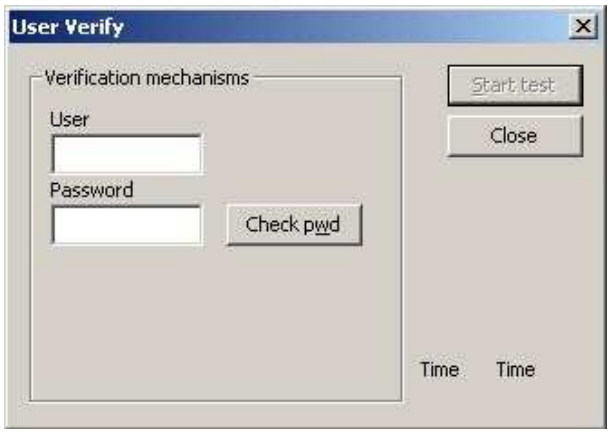

Figure 9: System 1: Username and password

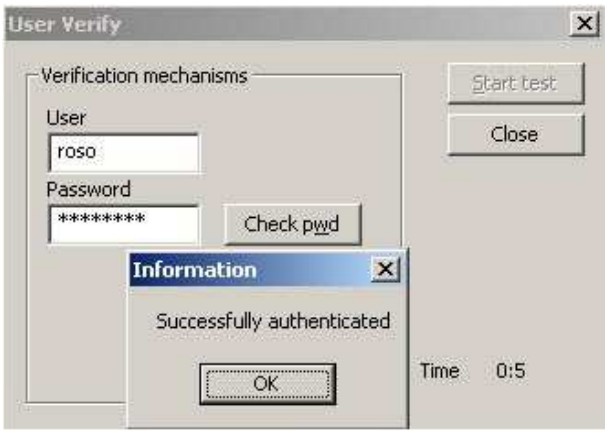

Figure 10: Successfully authenticated using username and password. Similar for the other systems.

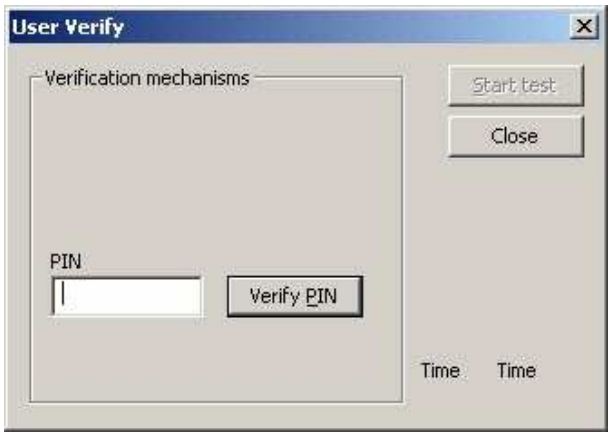

Figure 11: System 2: Smart card with PIN.

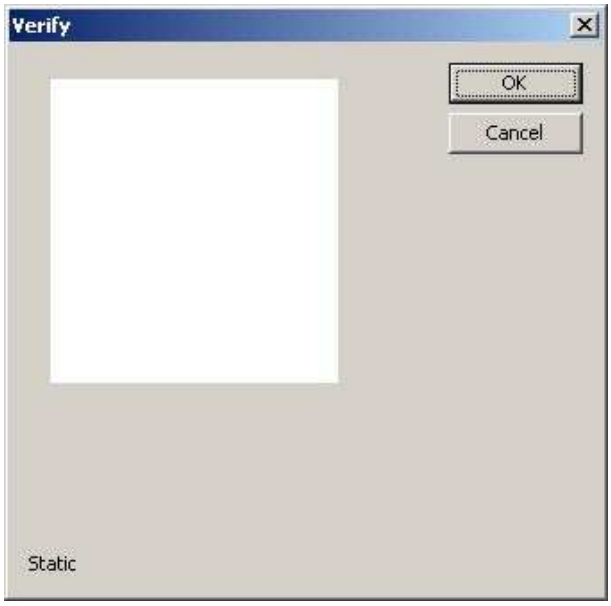

Figure 12: System 3: Fingerprint.

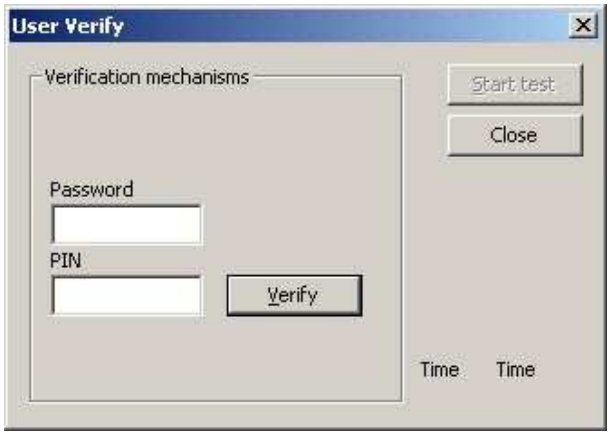

Figure 13: System 4: Password and smart card with PIN.

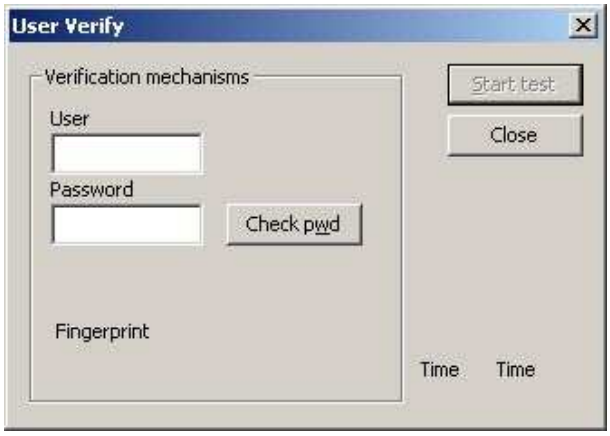

Figure 14: System 3: Fingerprint.

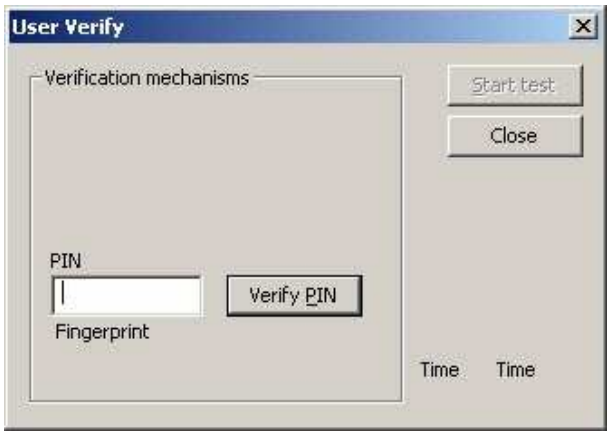

Figure 15: System 4: Password and smart card with PIN.

C Results from the experiment

The results from the experiment are summarized throughout this Appendix. Each authentication system has one table containing summary of the system separated questions in the questionary and one table containing ranking information from the summary questions in the questionary.

System 1- Username and Password

	1		2		3		4		5	
	#	%	#	%	#	%	#	%	#	%
Little/much effort.	40	65.6	17	27.9	4	6.6	0	0	0	0
Security for use in an industrial context, e.g. intranett.	0	0	2	3.3	11	18.0	17	27.9	31	50.8
Security regarding sensitive information and home use, e.g. online banking.	5	8.2	10	16.4	14	23.0	13	21.3	19	31.1
Usability in an industrial context.	0	0	1	1.6	10	16.4	22	36.1	28	45.9
Usability for home use.	0	0	2	3.3	8	13.1	24	39.3	27	44.3

Table 22: Table with summary of the questionary for the system 1.

Ranking from one to six, where one is the best. See question 15.

	Security		Usability		Home use		At work	
	#	%	#	%	#	%	#	%
1	1	1.7	5	8.3	14	23.3	4	6.7
2	2	3.3	18	30.0	20	33.3	15	25.0
3	1	1.7	21	35.0	12	20.0	8	13.3
4	1	1.7	9	15.0	3	5.0	6	10.0
5	14	23.3	3	5.0	4	6.7	9	15.0
6	41	68.3	4	6.7	7	11.7	18	30.0

Table 23: Ranking table for system 1, shows number and percentage of votes.

System 2- Smart Card with 4 Digit PIN

	1		2		3		4		5	
	#	%	#	%	#	%	#	%	#	%
Little/much effort.	46	75.4	11	18.0	2	3.3	0	0	2	3.3
Security for use in an industrial context, e.g. intranett.	0	0	3	4.9	7	11.5	19	31.1	32	52.5
Security regarding sensitive information and home use, e.g. online banking.	2	3.3	5	8.2	10	16.4	16	26.2	28	45.9
Usability in an industrial context.	0	0	3	4.9	4	6.6	20	32.8	34	55.7
Usability for home use.	0	0	3	4.9	5	8.2	21	34.4	32	52.5

Table 24: Table with summary of the questionary for system 2.

	Security		Usability		Home use		At work	
	#	%	#	%	#	%	#	%
1	0	0	1	1.7	3	5.0	5	8.3
2	0	0	30	50.0	17	28.3	12	20.0
3	1	1.7	15	25.0	15	25.0	13	21.7
4	14	23.3	9	15.0	15	25.0	15	25.0
5	35	58.3	5	8.3	7	11.7	11	18.3
6	10	16.7	0	0	3	5.0	4	6.7

Table 25: Ranking table for system 2, shows number and percentage of votes.

System 3- Fingerprint

	1		2		3		4		5	
	#	%	#	%	#	%	#	%	#	%
Little/much effort.	59	96.7	0	0	1	1.6	0	0	1	1.6
Security for use in an industrial context, e.g. intranett.	1	1.6	2	3.3	7	11.5	14	23.0	37	60.7
Security regarding sensitive information and home use, e.g. online banking.	4	6.6	2	3.3	6	9.8	15	24.6	34	55.7
Usability in an industrial context.	0	0	0	0	2	3.3	11	18.0	48	78.7
Usability for home use.	0	0	0	0	2	3.3	11	18.0	48	78.7

Table 26: Table with summary of the questionary for system 3.

	Security		Usability		Home use		At work	
	#	%	#	%	#	%	#	%
1	3	5.0	49	81.7	32	53.3	24	40.0
2	2	3.3	4	6.7	12	20.0	5	8.3
3	24	40.0	3	5.0	4	6.7	10	16.7
4	13	21.7	3	5.0	5	8.3	6	10.0
5	10	16.7	1	1.7	3	5.0	5	8.3
6	8	13.3	0	0	4	6.7	10	16.7

Table 27: Ranking table for system 3, shows number and percentage of votes.

System 4- Password and Smart Card with PIN

	1		2		3		4		5	
	#	%	#	%	#	%	#	%	#	%
Little/much effort.	15	24.6	18	29.5	18	29.5	9	14.8	1	1.6
Security for use in an industrial context, e.g. intranett.	1	1.6	3	4.9	6	9.8	18	29.5	33	54.1
Security regarding sensitive information and home use, e.g. online banking.	1	1.6	5	8.2	6	9.8	18	29.5	31	50.8
Usability in an industrial context.	3	4.9	12	19.7	15	24.6	12	19.7	19	31.1
Usability for home use.	3	4.9	10	16.4	14	23.0	13	21.3	21	34.4

Table 28: Table with summary of the questionary for system 4.

	Security		Usability		Home use		At work	
	#	%	#	%	#	%	#	%
1	2	3.3	1	1.7	2	3.3	3	5.0
2	9	15.0	0	0	1	1.7	5	8.3
3	18	30.0	5	8.3	7	11.7	11	18.3
4	30	50.0	18	30.0	18	30.0	12	20.0
5	1	1.7	13	21.7	14	23.3	15	25.0
6	0	0	23	38.3	18	30.0	14	23.3

Table 29: Ranking table for system 4, shows number and percentage of votes.

System 5- Username, Password and Fingerprint

	1		2		3		4		5	
	#	%	#	%	#	%	#	%	#	%
Little/much effort.	16	26.2	25	41.0	10	16.4	9	14.8	1	1.6
Security for use in an industrial context, e.g. intranett.	0	0	2	3.3	5	8.2	13	21.3	41	67.2
Security regarding sensitive information and home use, e.g. online banking.	0	0	1	1.6	3	4.9	21	34.4	36	59.0
Usability in an industrial context.	1	1.6	11	18.0	8	13.1	23	37.7	18	29.5
Usability for home use.	0	0	7	11.5	13	21.3	19	31.1	22	36.1

Table 30: Table with summary of the questionary for system 5.

	Security		Usability		Home use		At work	
	#	%	#	%	#	%	#	%
1	13	21.7	1	1.7	2	3.3	10	16.7
2	34	56.7	4	6.7	8	13.3	12	20.0
3	11	18.3	7	11.7	15	25.0	11	18.3
4	1	1.7	8	13.3	6	10.0	11	18.3
5	0	0	15	25.0	14	23.3	8	13.3
6	1	1.7	25	41.7	15	25.0	8	13.3

Table 31: Ranking table for system 5, shows number and percentage of votes.

System 6- Fingerprint and Smart Card with PIN

	1		2		3		4		5	
	#	%	#	%	#	%	#	%	#	%
Little/much effort.	24	39.3	28	45.9	7	11.5	2	3.3	0	0
Security for use in an industrial context, e.g. intranett.	0	0	2	3.3	5	8.2	11	18.0	43	70.5
Security regarding sensitive information and home use, e.g. online banking.	0	0	3	4.9	2	3.3	18	29.5	38	62.3
Usability in an industrial context.	1	1.6	2	3.3	11	18.0	21	34.4	26	42.6
Usability for home use.	0	0	6	9.8	7	11.5	26	42.6	22	36.1

Table 32: Table with summary of the questionary for system 6.

	Security		Usability		Home use		At work	
	#	%	#	%	#	%	#	%
1	41	68.3	3	5.0	7	11.7	15	25.0
2	13	21.7	4	6.7	3	5.0	11	18.3
3	5	8.2	10	16.7	6	10.0	7	11.7
4	1	1.7	13	21.7	13	21.7	9	15.0
5	0	0	22	36.7	18	30.0	12	20.0
6	0	0	8	13.3	13	21.7	6	10.0

Table 33: Ranking table for system 6, shows number and percentage of votes.