Method for evaluating authentication system quality

Morten Sporild

Master's Thesis
Master of Science in Information Security
30 ECTS
Faculty of Computer Science and Media Technology
Gjøvik University College, 2007

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

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

ABSTRACT

The purpose of authentication systems is to confirm a user's claimed identity. Authentication must also ensure that only persons with legitimate permissions are granted access. There are several ways of authenticating yourself, but common between all of them is that they use or combine at least one of the following principles; something one knows, something one has and something one is.

The aim of this thesis is to explore which authentication technologies large scale Norwegian enterprises make use of and if the system itself is good enough secured. Since one of the biggest dilemmas surrounding information security is the weighing between security and user-friendliness, this thesis will also try to discover if the usability is adequate, according to the user's perceptions, so that users will not be tempted into taking shortcuts that could compromise security.

The intention is also to examine if there is a way to measure authentication factors within security and user-friendliness with the use of metrics, and through this estimate how well the system works.

SAMMENDRAG

Autentiseringssystemer skal bekrefte at man er den man påstår man er, samt sikre at kun personer med rettmessig tilgang får aksess. Det finnes mange måter å autentisere seg på ovenfor et system. Felles for alle er at de benytter minst et av følgende prinsipper; noe man vet, noe man har og noe man er.

Hensikten med denne masteroppgaven er å undersøke hvilke autentiseringsteknologier større norske bedrifter benytter og om systemene rundt selve autentiseringen er godt nok sikret. Siden et av informasjonssikkerhetens store dilemmaer er avveiingen mellom sikkerhet og brukervennlighet, ønsker oppgaven også å finne ut om brukerne av de forskjellige systemene er fornøyd med bruken eller om terskelen for bruk ikke er så høy at de kan bli fristet til å ta snarveier som kan kompromittere systemes sikkerhet.

Bakgrunnen for oppgaven var også å undersøke om det finnes noen måte å måle autentiseringsfaktorer innenfor sikkerhet og brukervennlighet ved hjelp av metrikker, og gjennom dette beregne hvor godt systemet fungerer.

ACKNOWLEDGEMENTS

There are a number of people I would like to thank:

My supervisor, Slobodan Petrović, for his guidance during this thesis.

My employer Buypass AS, especially Sverre Sandernes, for grating me time to write this thesis while working full-time.

Chairman of the board at ISF, John A. Johansen, for his help in distributing the questionnaire to all members of ISF.

I would also like to thank all respondents of the questionnaire.

Table of Contents

List of tables

List of figures

1 INTRODUCTION

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

1.1 Problem Description

There are weaknesses concerning most systems for authentication. Several authentication methods like passwords, PIN-codes or smart-card authentication, without a combination of something one knows, can easily be exploited. Passwords are often based on words, and if users have too many of them, they tend to be written down and stored somewhere possibly unsafe. Proper user identification and authentication is a crucial part of the access control that makes the major building block of any system's security [1]. Well-implemented procedures for authenticating users can be seen as a first step of assuring the system's confidentiality in a society that is becoming more and more digitalized.

This thesis will try to discover to which extent it is possible to assess if one authentication system is better and more effective than another, and by doing that try to distinguish between good and bad security.

The purpose of any authentication system should be to make the authentication phase easy for the good guys and at the same time difficult to exploit by persons with malicious intents. This means one will have to consider aspects of both security and user-friendliness.

1.2 Topics covered by this thesis

This thesis will try to explore the conflict of interest between security and user-friendliness with regards to authentication systems. Its main focus will be to create a system of metrics for evaluating the effectiveness of various security measures and propose a system for ranking different authentication systems through vectors in a three dimensional space.

A survey among several large-scale Norwegian enterprises will also be carried out in order to produce statistical data and results that can be directly related to the proposed metrics and the research questions.

1.3 Justification, Motivation and Benefits

Authenticating users and verifying the identity of someone is very important. If security is compromised, privacy is likely to be compromised as well, as the whole information environment is based on trust [2].

Using metrics as a way of measuring information security, will better communication and decision making [3]. It will provide help in both determining the correct level of security and help direct resources to where they are most needed. Creating metrics for evaluating the quality of the implemented authentication system should provide useful information in determining if the system is good enough. This will help ensure that no unauthorized entities gain access to the system and prevent any breaches in the information security.

By presenting the results as vectors from an ideal point in a three dimensional space, we hope to ease how to interpret and compare the quantitative results from the metrics.

1.4 Research Questions

The following is a list of the research questions that will be discussed in this thesis:

- Which are the most preferred and most common authentication methods in large scale Norwegian enterprises and to what extent are several authentication mechanisms combined? Are the authentication systems properly secured?
- What are the user's perceptions on the level of user-friendliness using implemented authentication mechanisms?
- Is it possible to create a vector room with an ideal point, based on qualitative metrics, as a measure on how effective one's authentication system really is, and is this an expedient way of measuring?

1.5 Research Method

A quantitative research method seems to be an appropriate approach to answering the research questions in chapter 1.4. In [4] it is described that quantitative approaches are used where the investigator uses post positivist claims for developing knowledge. It also describes that a quantitative approach employs strategies of inquires such as experiments and surveys, and collects data on predetermined instruments that yield statistical data. The

purpose of this thesis is exactly that; to produce numerical statistical data with the use of metrics and questionnaires.

A literature study has also been performed in order to gain more in-depth knowledge of the use of metrics and the process on how they are created. A literature study of several authentication methods has been carried out to evaluate different authentication techniques with regards to security and usability. The work has also included theory about questionnaires and how they are created to produce the best possible result. All this theory will help to answer the research questions and act as a basis for conclusions.

2 PREVIOUS WORK

This chapter contains a literature study of the areas related to the research questions in chapter 1.3.

Security is only one of many considerations when it comes to designing a system. It is a trade-off between cost, benefit and flexibility as well. The author Odlyzko [5] states that lack of perfect security is not likely to be fatal and it is often enough to be sufficiently secure. The article uses the analogy, that security should be like speed bumps; decrease velocity and impact such that other mechanisms can operate.

2.1 Authentication methods - security and user-friendliness

Authentication is the binding of an identity to a subject. Basically there are three ways of authenticating someone: by something one knows, by something one has and by something one is [6]. Some people even add a forth, authentication based on where one is [7].

Something one knows is generally a password, PIN code or any other secrets. The objective of this method is that a person proves ownership of a hard-to-guess secret to the target computer. The main vulnerability with this kind of authentication is therefore that someone e.g. the verifier can learn your secret. If the users are free to choose their own passwords they tend to choose passwords that are easy to remember and easy to guess, thus failing to provide adequate protection.

This article [8] discusses the evolution of password policies and the notion of good passwords. The evolution has gone from "Each password you choose must be new and different" through "Passwords must be memorized. If a password is written down, it must be locked up", "Passwords must be at least six characters long, and probably longer, depending on the size of the password's character set", "Passwords must be replaced periodically" to "Passwords must contain a mixture of letters (both upper- and lowercase), digits, and punctuation characters". The article provides an overview of the growth of percentage of passwords found by systematic searches or brute force attempts. This number has grown from 24 percent in the 1990's to over 35 percent in 2000, as computational power has increased. There is nothing productive or entertaining about memorizing obscure passwords, but is seems to be a matter of necessity if this method for authenticating users alone should be used at all.

Something one has includes objects like smart cards, RFID-chips (Radio Frequency Identification) [9], one-time password/code generators (like the ones many banks equip customers with) or other similar objects. This form of authentication is also vulnerable as objects can be stolen. One-time-passwords are also vulnerable to phishing and man in the middle attacks, like there have been some examples of lately with internet banking. This category is often subject to high cost implementation as each user will need some type of hardware, especially so with smart cards and smart card readers.

Something one is, is considered the most difficult method to forge, but not impossible as this fingerprint article provides evidence of [10]. Biometrics have an advantage over passwords and tokens as they cannot be forgotten, even though they can be lost with damage to one's physical appearance. The second problem of biometrics is, as stated above, that even though it might be a unique identifier, it is not a secret. There are several ways of using a person's biometrics, as the body contains several physical features suitable for unique identification.

Biometric authentication can use several human properties for identification [11] and [12]:

- DNA: Deoxyribo Nucleic 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, but can be 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 [13].
- Gait: The peculiar way one walks. This is however behavioral dependent and might not stay invariant over time [14].
- 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 persons wearing eyeglasses.
- 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. Just like iris scan, this can also be inconvenient for persons wearing eyeglasses.

- Keystroke dynamics: There is a hypothesis that each person types on a keyboard in a characteristic way. This behavior is heavily influenced by injuries, sickness and emotions and could prove to be easily forged.
- Odor: Each person odors a chemical characteristic. Affected by environment, type of food eaten, deodorant used or similar.
- Signature: The way a person signs his/her name. Behavioral influenced by emotions and may change over time. This property can also be behaviorally influenced by injuries, sickness and emotions.
- Voice: Voice capture is unobtrusive and an acceptable biometric, but one problem though is mimicking vulnerabilities.

The article [15] discusses the usability and acceptability of biometric security systems. Biometric authentication systems have gained a lot of attention lately because of the potential to increase the accuracy and reliability of identification and authentication. The latest focus has concerned the use of biometrics in passports [16]. A lot of research has been done to assess the performance of biometric systems, with an emphasis on false acceptances and rejections. Much less research has been done on the usability and acceptability of biometric security systems when used by IT professionals and the general public. Several factors have increased the usability of using biometrics for authentication as the sensors keep getting smaller, become more reliable and keep getting implemented in new state of the art technology. The biometric algorithms themselves also keep getting better. However there are still some usability concerns like accuracy, awkward use (iris, retina scanners) and intuitiveness.

The article in [1] discusses where biometric authentication will be beneficial and where it will not. Even cheap and simple biometric solutions can increase the overall system security if used on top of existing traditional authentication methods. The article offers some basic conclusions:

- Different biometric samples of the same person will never be same.
- Biometric systems make errors.
- Biometric data are not secret.
- The role of the input device is crucial and this device must be trusted or well secured.
- The biometric system should check user's liveness (verify whether or not the biometrics are from a living person).
- Biometrics are good for user authentication, however they cannot be used to authenticate data or computers.

The article in [17] concerns the security and usability regarding basic authentication methods and includes a discussion of pros and cons with the different methods. The author concludes that pure password authentication should be replaced and that expectations are that the use of smart cards will continue to rapidly increase in the future.

The authors of the article in [18] are investigating the techniques and methods for enhancing user-centered security. Usability and security must be merged in order to develop acceptable systems that will not be disregarded by legal or non-legal users.

Authentication is not the end itself [2]. In general, people are authenticated so that their request to do something can be authorized and be held accountable (non-repudiation).

2.2 Measuring performance and developing metrics

NIST 800-55 Security Metrics for Information technology Systems is a guide on how an organization through the use of metrics, identifies the adequacy of in-place security controls, policies and procedures. It provides help for management to decide where to invest in additional security protection resources or identify and evaluate non-productive controls [19]. The article provides a step by step guide on the metric development and implementation process, and describes techniques that will help developing metrics that identify poor performance.

According to the authors these matters must be considered during development and implementation of IT security metrics:

- The metrics must produce quantifiable information, such as percentages, averages and numbers.
- Data that is used as input to the metrics must be readily obtainable.
- Only repeatable processes should be used and measured.
- Metrics must be useful for routing resources and trace performance.

A metric program should according to this NIST publication include these four independent components:

Figure 1 - Metric components

- Strong upper level management which is critical for a successful implementation of a metrics program.
- Practical security policies and procedures, or else the metrics are not easily obtainable.
- Quantifiable performance metrics must be defined so that they capture meaningful performance data.
- Result-oriented metric analyses: The program must stress a periodic analysis of the metric data, for the program to be successful.

The authors of the article in [20] emphasizes that there is no known algebra for security. Important factors when creating metrics include:

- Scope must be clearly characterized.
- Must have a solid foundation.
- The metric assessment process must be well defined.
- The metrics must be repeatable and reproducible with the same results.

The article also divides metrics into several categories: objective or subjective, quantitative or qualitative, static or dynamic, absolute or relative and direct or indirect. It also discusses cost benefits of different authentication mechanisms.

In [21], there is a call for quantifiable measures for information security. Usage related vulnerabilities will still remain even if software is secure.

The author of the article in [22] does not believe in numerical measures for information assurance, but would rather consider the key factors in information security; confidentiality, integrity, availability, authentication and non-repudiation. In contrast to a lot of other authors, he believes that 80% security is hardly good enough. The goal should be 99, 99%. The author then proposes a "Resilience Assurance Index (RAI)", which correlates events on information warfare timeline and countermeasures; protection, detection and reaction.

In "Security metrics from a management perspective" [23] Frost describes the process of defining metrics. This author focuses on creating and implementing metrics in a management context. He stresses that the number of metrics should be kept to a minimum, even though one have to make sure that all important aspects should be included in the measurements.

A "three step method" is created for a top down procedure for development**.** This top down procedure for developing metrics contains identification of:

- Performance topics: Confidentiality, integrity, availability and recovery
- Critical success factors for each topic: You need well defined and well understood definitions of the performance topics, effective procedures and processes and trustworthy technology.
- Performance indicators for each success factor.

Various surveys indicate that over several of the past years, computer security has risen in priority for many organizations [24]. This leads to larger budgets for the computer security area within companies, with a demand for return of investment by the management. The author claims that experts suggest the key to achieving that is by the use of security metrics. The article contains a guide that provides a definition of security metrics, explains their value, discusses the difficulties in generating them, and suggests a seven-step methodology for building a security metrics program. The author states that it helps to understand what metrics are, by drawing a distinction between metrics and measurements. Measurements provide single-point-in-time views of specific, discrete factors, while metrics are derived by comparing to a predetermined baseline two or more measurements taken over time. Metrics are an effective tool for those who work with security, especially

to discern the effectiveness of different security components, products, systems or processes. Metrics can also help identify the level of risk in not taking a given action, and in that way provide guidance in prioritizing corrective actions. Creating useful metrics should help answering questions on whether one is more secure than before, how one compares with others in regard to security and understand if one is secure enough. Good metrics are those that are SMART; Specific, Measurable, Attainable, Repeatable and Time-dependent.

3 PROPOSED METRICS FOR EVALUATING AUTHENTICATION SYSTEM QUALITY

3.1 Metric template

Information security is almost always a trade-off between security and user-friendliness. The metrics and discussion in this chapter is therefore divided into the two categories. Section 3.2 defines the metrics for authentication security, while 3.3 define metrics for user-friendliness.

In the process of defining the metrics, the guideline in NIST 800-55 Security Metrics for Information technology Systems as a guideline [19] has been utilized (ref. Chapter 3.2). Some minor adjustments has been made to the baseline in this guide, as there are two types of errors that can affect empirical measurements; random and non-random errors. Reliability and validity have been added to help measure the completeness and correctness of the metrics.

Fundamentally, reliability concerns the extent to which an experiment, test, or any measuring procedure yields the same results on repeated trials [25]. The reliability aspect has therefore been added to ensure that the metrics are created, so that the result they produce can be recreated. However it is important to note that one test can never be exact like another, as unreliability is always present to at least a limited extent.
This means that the index of variation (IV) should be as small as possible.

IV = Standard deviation / mean

Possible methods for ensuring reliability in empirical data could include:

- Retest method: the same test is given to the same people after a period of time.
- Alternate form method: test the same people that performed the first test for the same thing, but with an alternate form.
- Split-halves method: the total set of items is separated into two halves and the scores of each half are correlated to obtain an estimate of reliability.

Adding validity to the metrics will help ensure that we measure what we think we are measuring and what we are intending to measure. While reliability concerns the possibility of random errors, validity deals with removing systematic errors from the measurement, as errors in the measuring instrument, here the metrics.

Validity is a matter of degree, not an all or none property. Just because an indicator is quite reliable it does not mean that it is relatively valid [25].

There are three types of validity that can affect the measurements:

- Construct validity: The extent to which the translation of a construct/concept to its operationalization is valid.
- Criterion related validity (predictive validity): The correlation with a measurement of a different variable, which more closely corresponds to what we want to measure.
- Content validity: The degree of completeness in the operationalization.

Table 1 shows the metric template that has been used during the metric development process.

Table 1 - Metric template

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 metrics are implemented.
Performance Objective	Description of actions required to accomplish the performance goal.
Metric	Description of what we are measuring with the metric.
Purpose	The goal of this metric.
Implementation evidence	Tasks and sub-questions to help measuring the critical element.
Frequency	How often the metric is conducted, during a period of specified time.
Formula	Describe 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. Will the metric produce the same results on repeated trials?
Validity	The degree of completeness of this metric. Are the measurements designed in such way that our measurements give a fair picture of the variable being measured? Do the measurements reflect what they are supposed to or are they influenced by the operation of contaminating factors?

3.2 Metrics for authentication system security

3.2.1 Metric M-1 – Authentication method

Table 2 defines the first metric M-1 – Authentication method. The purpose of this metric is to determine which authentication methods are implemented and provide a quantitative result, based on the level of security for the respective authentication method. The ranking of systems and formula in this metric is based on findings in [11].

Table 2 - Metric M-1 - Authentication Method

Metric ID	**M-1**
Name	Authentication method.
Performance Goal	Determine what kind of authentication method(s) is/are implemented.
Performance Objective	Are effective authentication methods implemented?
Metric	Determine the security level of implemented authentication methods.
Purpose	Determine which authentication methods are implemented and provide a quantitative result based on the level of security for each authentication method.
Implementation evidence	Does the system use authentication methods based on: • No authentication Yes ☐ No ☐ • Pin/Password, something you know Yes ☐ No ☐ • Smartcard or one-time password, something you have Yes ☐ No ☐ o In combination with secret? o Yes ☐ No ☐ • Biometric authentication, something you are Yes ☐ No ☐ • Other Yes ☐ No ☐ Description [ ]
Frequency	Yearly

<table>
<tr><td>Formula</td><td>
<table>
<tr><td>No authentication</td><td>0 points</td></tr>
<tr><td>Username/password</td><td>1 point</td></tr>
<tr><td>Smart card authentication</td><td>1 point</td></tr>
<tr><td>Biometric authentication</td><td>2 points</td></tr>
<tr><td>Smart card/secret combination</td><td>3 points</td></tr>
<tr><td>One-time passwords (OTP)/secret combination</td><td>3 points</td></tr>
<tr><td>Smart card/biometric combination</td><td>4 points</td></tr>
<tr><td>Combination of something you know, have and are</td><td>5 points</td></tr>
</table>
</td></tr>
<tr><td>Data source</td><td>System documentation</td></tr>
<tr><td>Indicator</td><td>This metric will provide the security effectiveness of authentication methods</td></tr>
<tr><td>Reliability</td><td>The possibility for random errors with this metric is small. System documentation should provide information necessary.</td></tr>
<tr><td>Validity</td><td>This metric should provide valid results.</td></tr>
</table>

The reason why smart card authentication and biometric authentication alone is ranked differently, even though they both use only one authentication method, is that it is considered easier to steal a smart card from somebody than it is to fake a biometric property. The same reasoning applies to a smart card/biometric combination contra OTP/secret combination and smart card/secret. A combination of all three authentication techniques is considered most secure and is therefore awarded with a full score of five points.

3.2.2 Metric M-2 – Client server communication – cryptographic encryption and authentication quality.

Communication over insecure lines needs to be authenticated and encrypted. Recommended key lengths vary over time as computational power increase. As stated in ECRYPTY early Report on Algorithms and Key sizes, industry experts seem to agree that it is likely that Moore's law will continue to apply for at least a decade or more [26]. The points given in metric M-2 are therefore based on these assumptions with respect to adversary capabilities.

Table 3 from NIST 800-57 [27] describes the algorithms and key sizes that are considered appropriate for the protection of data from 2007 and beyond 2030.

Table 3 - Recommended algorithms and minimum key sizes NIST 800-57

Algorithm security lifetimes	Symmetric key algorithms	FFC (e.g., RSA and D-H)	IFC (e.g., RSA)	ECC
Through 2010 (min. of 80 bits of strength)	23 2TDEA 3TDEA AES-128 AES-192 AES-256	Min.: L = 102 N =160	Min.: k=1024	Min.: f=160
Through 2030 (min. of 112 bits of strength)	3TDEA AES-128 AES-192 AES-256	Min.: L = 2048 N = 224	Min.: k=2048	Min.: f=224
Beyond 2030 min. of 128 bits of strength)	AES-128 AES-192 AES-256	Min.: L = 3072 N = 256	Min.: k=3072	Min.: f=256

Explanation to table 3 "Recommended algorithms and minimum key sizes NIST 800-57":

- Column 1: Indicates the time periods the specified cryptographic algorithms are considered secure.
- Column 2: Identifies appropriate symmetric key algorithms and key sizes. 2TDEA and 3TDEA are specified in [28], the AES algorithm is specified in [29], and the computation of Message Authentication Codes (MACs) using block ciphers is specified in [30].

- Column 3 indicates the minimum size of the parameters associated with Finite Field Cryptology (FFC), such as DSA as defined in [31].
- Column 4 indicates the minimum size of the modulus for integer factorization cryptography (IFC), such as the RSA algorithm specified in [32].
- Column 5 indicates the value of f (the size of n, where n is the order of the base point G) for algorithms based on elliptic curve cryptography (ECC) that are specified for digital signatures and for key establishment as specified in [33]. The value of f is commonly considered to be the key size.

One point in table 4 corresponds to a key size that should provide protection from year 2007 – 2010 according to [34], which has been used as a basis for the key size score in metric 2 together with [35]. Two points corresponds with a protection until year 2015. E.g. upper bound one point will provide resistance until year 2010 with a minimum of 73-bit key for symmetric systems like AES-128 [36] and a minimum of 1376-bit key for asymmetric systems like RSA [36].

In table 4 SDL is short for subgroup discrete logarithm systems, while ECC is short for elliptic curve cryptography systems.

Table 4 - Score table for metric M2

Points	Symmetric key size	Asymmetric key size	SDL key size	Hash key size (ECC)
0	0-73	0-1037	0-146	0-146
0.5	73-75	1037-1112	146-150	146-150
1	75-78	1112-1245	146-156	146-156
1.5	> 78	> 1245	> 156	> 156

Table 5 defines the metric for secure client-server communication between the authenticating client and the server receiving the authenticating data based on cryptographic encryption and authentication quality as well as key lengths.

Table 5 - Metric M-2 - Client server communication – cryptographic encryption and authentication quality

<table>
<tr><th>Metric ID</th><th>M-2</th></tr>
<tr><td>Name</td><td>Client server communication – cryptographic encryption and authentication quality.</td></tr>
<tr><td>Performance Goal</td><td>Determine cryptographic strength in the communication and authentication between servers to avoid tampering.</td></tr>
<tr><td>Performance Objective</td><td>Investigate if the client-server communication is properly secured.</td></tr>
<tr><td>Metric</td><td>Are secured communication channels implemented, and to which extent are the algorithms and lengths of keys good enough?</td></tr>
<tr><td>Purpose</td><td>Determine if the communication environment is properly secured, with the use of communication encryption.</td></tr>
<tr><td>Implementation evidence</td><td>Is the communication secured using:

• Encryption in client – server connection
Yes ☐ No ☐
• Authentication in client – server connection
Yes ☐ No ☐

If implemented:
• Type of encryption algorithm:
[ ]
• Size of key:
[ ]

• Type of authentication algorithm:
[ ]
• Size of key:
[ ]</td></tr>
<tr><td>Frequency</td><td>Once yearly</td></tr>
<tr><td>Formula</td><td><table>
<tr><td>No encryption or authentication</td><td>0 points</td></tr>
<tr><td>Encryption algorithm</td><td>1 point</td></tr>
<tr><td>Authentication algorithm</td><td>1 points</td></tr>
<tr><td>Key size</td><td>0-1.5 points for encryption key size
0-1.5 points for authentication key size</td></tr>
</table></td></tr>
</table>

	Proprietary algorithms. No points for key size.	1 point
Data source	System documentation	
Indicator	This metric will provide the strength of implemented encryption and authentication algorithms.	
Reliability	The possibility for random errors with this metric is small. System documentation should provide information necessary.	
Validity	Systems that use proprietary algorithms will be difficult to measure. Such cases will affect the validity of this metric.	

One point is given when proprietary algorithms are used, but gain no points for key size. The reasoning for this is that a proprietary algorithm can be hard to break, but the quality is impossible to assess. It should however be awarded for effort even though security by obscurity is generally a bad idea.

The systems should also be evaluated according to ITSEC [37] or Common Criteria [38], even though the encryption might be sufficiently strong, to make sure the environment and encapsulation of data is implemented securely. This is however not a part of the indicators for this metric.

3.2.3 Metric M-3 – Secure log-on associated procedures

The metric in table 6 is based on log-on security associated requirements in ISO/IEC-17799 [39], which is a standard for information security with recommendations made for persons responsible for creating, activating and maintaining security related work within organizations. This metric is created of indicators that should determine if the system's access control is properly secured through implemented procedures.

Table 6 - Metric M-3 - Secure log-on associated procedures

Metric ID	**M-3**
Name	Secure log-on associated procedures
Performance Goal	Determine if the system's access control is properly secured through procedures.
Performance Objective	Investigate if the authentication system has secure procedures.
Metric	Provides a measurement of associated procedures.
Purpose	Determine the use of superior procedures surrounding the authentication system

Implementation evidence	Is the log on procedure associated with the authentication secured with the following techniques: • If error condition arises, the system does not indicate which part of the data is correct or un-correct. Yes ☐ No ☐ • Limit number of unsuccessful logon attempts with one or more of the following consequences; time delay until next possible authentication attempt, recording unsuccessful attempts, disconnect connection, alarm trap: Yes ☐ No ☐ • Limit the maximum allowed log-on time: Yes ☐ No ☐ • Does the system display the following information on completion of successful authentication attempts: Date and time of last successful authentication and detail on any unsuccessful attempts: Yes ☐ No ☐ • All users have their own unique identifier which is for personal use only: Yes ☐ No ☐
Frequency	Once yearly
Formula	One point for each implemented procedure, with a maximum of 5 points. If the procedure is not relevant as with implementation evidence 1 and biometrics, a point is awarded nevertheless.
Data source	System documentation
Indicator	This metric will provide the strength of procedures surrounding the authentication/log-on phase.
Reliability	The possibility for random errors with this metric is small. System documentation should provide information necessary.
Validity	This metric should provide a fair picture of what we are trying to measure. However these 6 questions will not provide a complete spectrum of objects regarding log-on security, as they are only 6 of several security indicators on this subject.

	Too few indicators can affect the validity negatively.

3.3 Metrics for User-friendliness

User-friendliness can be defined as a set of attributes that bear on the effort needed for use, and on the individual assessment of such use, by a stated or implied set of users [40]. ISO-9126 defines indicators like learnability, understandability and operability. ISO 9241-11 [41] defines usability as the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use. These indicators have been used as a basis for the user-friendliness metrics in M-4, M-5 and M-6,

3.3.1 Metric M-4 – Authentication method - user friendliness

Metric M-4 uses the same indicators as M-1 but the formula is based on the level of user-friendliness. These rankings are also based on the findings in [11] and the formula accordingly.

The reasoning for giving smartcard/biometric combination 2 points while smartcard secret/combination 1 point, even though they both combine two authentication methods, is also based on those findings of perceived usability. It seems like it is perceived as easier to use something one don't have to remember, like a biometric feature, instead of having to remember a secret in combination together with bringing a smartcard. A smartcard alone (3 points) is also awarded less than biometric alone, as there is no need to remember to bring something with you to be authenticated.

The results from the study in [42] show that end-users accept biometric authentication systems easily, without much concern for security or concern for storing of one's biometric characteristics. If this was not the case, biometric authentication alone should not have been awarded four points in the formula.

Table 7 - Metric M-4 - Authentication method - user friendliness

Metric ID	**M-4**
Name	Authentication method - user friendliness
Performance Goal	Determine what kind of authentication method(s) is/are implemented.
Performance Objective	Are user-friendly authentication methods implemented?
Metric	Determine the level of user-friendliness in implemented authentication methods.
Purpose	Determine which authentication methods are implemented and provide a quantitative result based on the level of usability for each authentication method.
Implementation evidence	Does the system use authentication methods based on:

<table>
<tr><td></td><td>

No authentication
Yes ☐ No ☐
Pin/Password, something you know
Yes ☐ No ☐
Smartcard or one-time password, something you have
Yes ☐ No ☐

In combination with secret?
Yes ☐ No

Biometric authentication, something you are
Yes ☐ No ☐
Other
Yes ☐ No ☐
Description [ ]

</td></tr>
<tr><td>Frequency</td><td>Yearly</td></tr>
<tr><td>Formula</td><td>
<table>
<tr><td>No authentication</td><td>5 points</td></tr>
<tr><td>Biometric authentication</td><td>4 points</td></tr>
<tr><td>Smartcard authentication</td><td>3 point</td></tr>
<tr><td>Smartcard/biometric combination</td><td>2 points</td></tr>
<tr><td>Username/password</td><td>1 point</td></tr>
<tr><td>OTP/secret combination</td><td>1 point</td></tr>
<tr><td>Smartcard/secret combination</td><td>1 points</td></tr>
<tr><td>Combination of something you know, have and are</td><td>0 points</td></tr>
</table>
</td></tr>
<tr><td>Data source</td><td>System documentation and surveys.</td></tr>
<tr><td>Indicator</td><td>This metric will provide the level of user friendliness of authentication methods.</td></tr>
<tr><td>Reliability</td><td>The reliability will depend on sample size, in this case, the number of people that have answered. A larger sample size will help wash out variation that is naturally present in subjective answers like this.</td></tr>
<tr><td>Validity</td><td>Prior knowledge by the people participating in the survey on what the different authentication mechanisms are, could affect the validity of this metric</td></tr>
</table>

3.3.2 Metric M-5 – Authentication method - ease of use

The metric defined in table 8 aims to measure the user's subjective opinion on how easy their respective authentication method is to use.

Ease of use refers to the property of a product or thing that a user can operate without having to overcome a steep learning curve. Things with high ease of use will be intuitive to the average user in the target market for the product. The term is often used as a goal during the design of a product, as well as being used for marketing purposes. Put simply, things with "high ease of use" are easy to use. However, some experts distinguish ease of use from ease of learning, especially when the design of a product involves a trade-off between the two goals, or between ease of use and other goals such as security.

Indicators taken into account are the difficulties, or lack thereof, in learning how to use the system and if it is intuitive. If the learning phase takes too long or the system is simply too advanced to use, many users will resist using it. This could potentially result in shortcuts being made, which in turn could prove to be breaches in security. The metric in M-5 also asks the users to consider the rate of errors while trying to authenticate themselves.

Table 8 - Metric M-5 - Authentication method – ease of use

Metric ID	**M-5**
Name	Authentication method – ease of use
Performance Goal	Measure if the system is easy to use without having to overcome a steep learning curve.
Performance Objective	Determine the effort it takes for new and existing users to operate the authentication procedure.
Metric	Effort of learning and using the system.
Purpose	Measure the effort needed to learn and be comfortable with the system.
Implementation evidence	Measure the user's opinion of the learning curve and the ease of use once initial learning phase has stopped. Learning curve: Easy 2,5 ☐ 2 ☐ 1,5 ☐ 1 ☐ 0,5 ☐ 0 ☐ Difficult Use, once the initial learning phase has stopped, consider the rate of errors when answering this question (errors also includes forgetting a secret like PIN or password): Easy 2,5 ☐ 2 ☐ 1,5 ☐ 1 ☐ 0,5 ☐ 0 ☐ Difficult

Frequency	Once per person
Formula	Addition of points from both items in implementation evidence.
Data source	User opinions.
Indicator	An important factor of the system's user-friendliness.
Reliability	The effort needed to learn systems can depend on the user's previous or similar knowledge. The reliability will also depend on sample size, in this case, the number of people that has answered. A larger sample size will help wash out variation that is naturally present in subjective answers like this.
Validity	The validity of this metric should be very good as we only measure people's views on the subject. What could downgrade the validity is a failure to understand the questions by the participants. This way this metric will not measure what it is supposed to.

3.3.3 Metric M-6 – Authentication method - speed of performance

Speed of performance is closely attached to metric 5, ease of use, and is very important when dealing with often impatient users. This metric M-6 aims to measure the time it takes to authenticate and determine to which degree the users find the time consumption acceptable, which becomes basis for the resulting score.

User feed-back during the wait period is a key to decreasing perceived time consumption.

Table 9 - Metric M-6 - Authentication method – speed of performance

Metric ID	**M-6**
Name	Authentication method – speed of performance
Performance Goal	Measure if the time it takes to authenticate using the system, appears acceptable to the users.
Performance Objective	Determine if the authentication process takes an excessive amount of time, after the initial learning phase has stopped.
Metric	Time consumption.
Purpose	Measure the time it takes to authenticate using the system.
Implementation evidence	Measure the user's perception on acceptable time consumption for the authentication process. Authentication phase • In seconds [ ]

	User's rating • Not acceptable 0 ☐ 1☐ 2☐ 3☐ 4☐ 5☐ Acceptable
Frequency	Once per person
Formula	Points according to the Implementation evidence
Data source	User's opinion of the time consumption in the authentication phase.
Indicator	User's opinion.
Reliability	The user's understanding of authentication mechanisms and overall understanding of security, might affect the results of this metric. The reliability will also depend on sample size, in this case, the number of people that has answered. A larger sample size will help wash out variation that is naturally present in subjective answers like this.
Validity	The validity for this metric should be very good as we measure the users' perceptions only.

Both metric M-5 and M-6 are created with a pre-defined set of alternatives for the users to choose from. Otherwise the users' subjective opinions can be difficult to rank or measure.

4 RESULTS IN VECTORIAL FORM

All the metrics in chapter 3 are created with a maximum score of 5 points. This way there is no need for matching the score distribution to a common domain or use score normalization [43].

To evaluate which system is better based on the output of the metrics, their score will be added to two three-dimensional vectors, representing each of the two categories. The result from each metric's formula represents the value or size of the x, y and z values in a three-dimensional system.

We define:

S (Security) as the metrics M-1, M-2 and M3.

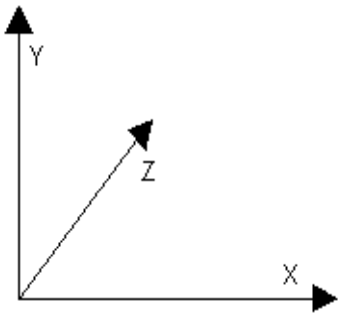
$S = (M1_x, M2_y, M3_z)$

U (User-friendliness) as the metrics M-4, M-5 and M-6

$U = (M4_x\ M5_y, M6_z)$

An ideal result for all the metrics created, is 5 points. This way an ideal score is represented as a vector running from $(0_x, 0_y, 0_z)$ to $(5_x, 5_y, 5_z)$.

$I = (5_x\ 5_y, 5_z)$.



The systems can then be evaluated for each of the two categories S and U as the distance between S and U with vector I. The shorter the distance between the vector S or U and vector I, the better the system is according to the indicators in the proposed metrics.

This distance, d, in three-dimensional space can be calculated with the use of Euclidean distance. Euclidean distance can be used with both discrete and continuous coordinates. This formula is therefore applicable in our case with discrete coordinates, even though distance is continuous.

$$Distance: d = |x - y| = \sqrt{\sum_{i=1}^{n} |xi - yi|^2}$$

In our case this means:

$$Distance\ between\ I\ and\ S:\ d = \sqrt{(Ix - M1)^2 + (Iy - M2)^2 + (Iz - M3)^2}$$

$$Distance\ between\ I\ and\ U: d = \sqrt{(Ix - M4)^2 + (Iy - M5)^2 + (Iz - M6)^2}$$

Or:

User-friendliness: $d = \sqrt{(5 - M1)^2 + (5 - M2)^2 + (5 - M3)^2}$

Security: $d = \sqrt{(5 - M4)^2 + (5 - M5)^2 + (5 - M6)^2}$

5 EXPERIMENT AND RESULTS

5.1 Experiment

A survey has been created to explore which authentication techniques are used at a number of large-scale Norwegian enterprises. The survey was defined to investigate authentication techniques and procedures regarding log-on to users' workstations and consists of two parts. Part one was made for system administrators or system owners, while part two was made for the users and wish to investigate their perceptions concerning the use of the system. This separation reflects the two categories of metrics presented in chapter 3.

The survey was created with as much fixed respondents or predefined answers as possible. This method makes it easier to interpret the answers subsequently. The questionnaire was also attempted made as simple as possible to make it easier for the respondents to understand the questions and hopefully generate more responds than if the questions were too incomprehensible.

The population for this questionnaire was large-scale Norwegian enterprises. Our definition of large scale in this setting was enterprises with more than 100 employees.

The questionnaire in appendix A was originally sent by mail to 40 large scale companies in Norway, but this method didn't produce more than two responses. The questionnaire was therefore recreated as a web form and published on http://sporild.com/. It was presented via php-scripts and the respondents' results were saved in a mysql database for further analysis.

A link to the digitalised survey was then sent to all members of ISF [44], by the leader of the board John A. Johansen, as a part of an e-mail with information about the next member meeting. ISF is an ideal organization working with information security in Norway. The members include organizations from public administration and private industry and commerce. The list of recipients included over 400 persons and produced results from 17 different large scale companies. Our selection, out of the population for the questionnaire, was therefore members of ISF.

This web based questionnaire (in Norwegian) is also presented in appendix A.

5.2 Results part 1

Figure 2 presents the scores in metric M-1 for the 17 respondents of part one of the questionnaire. A maximum result according to metric formula in M-1 for security is 5 points. Figure 3 presents an overview of the results per category.

The arithmetical average in the survey was a score of 2.059 and the mean was one point.

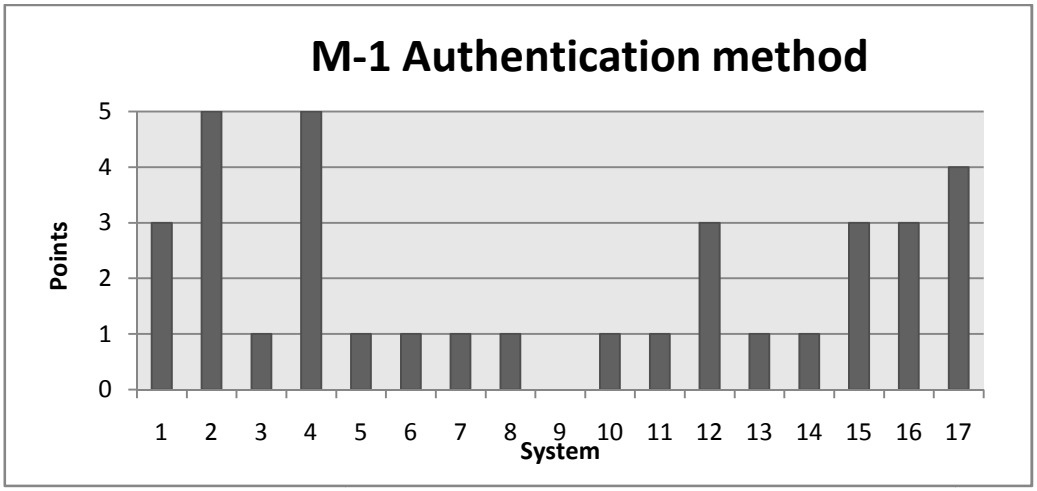


Figure 2 - Results M-1 – Column chart

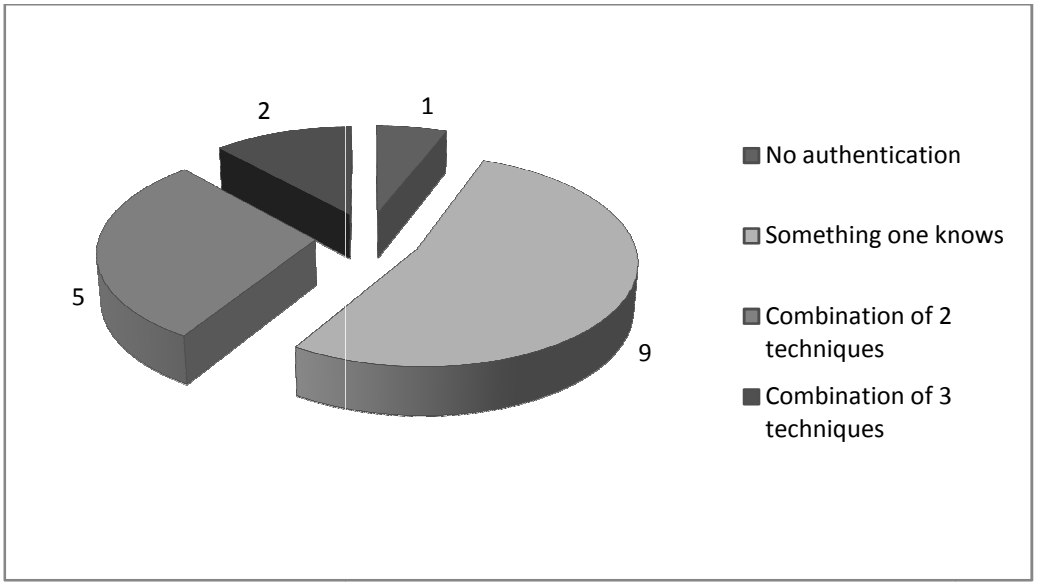


Figure 3 - Results M-1 – Pie chart

Table 10 displays the specific answers of M-1 for all 17 companies in the survey.

The values for "Authentication method(s)" are explained and presented in table 11.

System Number	Number of employees	Authentication method(s)
1	100 – 1000	2 and 3
2	100 – 1000	2, 4 and 5
3	100 – 1000	2
4	1000 +	2, 3 and 5
5	1000 +	2
6	1000 +	2
7	1000 +	2
8	1000 +	2
9	100 – 1000	1
10	100 – 1000	2
11	100 – 1000	2
12	100 – 1000	2 and 3
13	100 – 1000	2
14	100 – 1000	2
15	100 – 1000	2 and 4
16	100 – 1000	2 and 3
17	1000 +	3 and 5

Table 10 - Authentication methods

Authentication method	Representing value
No authentication	1
Something you know, PIN/password	2
Something you have, smart card	3
Something you have, OTP	4
Something you are, biometrics	5
Other	6

Table 11 - Authentication method - representing value

Table 12 presents the score results from part one of the questionnaire. The system's individual ranking can be seen in the column "Euclidean distance from I". According to the method described in chapter 4, a lower result indicates a point closer to the ideal. The complete overview of the results from the questionnaire can be found in appendix B.

System	Result M-1	Result M-2	Result M-3	Euclidean distance from I
1	3	2,5	2	4,387
2	5	2,5	3	3,202
3	1	3,5	2	5,220
4	5	5	4	1,000
5	1	2	3	5,385
6	1	0	3	6,708
7	1	0	4	6,481
8	1	5	3	4,472
9	0	1	1	7,550
10	1	1	5	5,657
11	1	0	3	6,708
12	3	2,5	4	3,354
13	1	0	3	6,708
14	1	2,5	4	4,822
15	3	5	2	3,606
16	3	2,5	3	3,775
17	4	3,5	3	2,693

Table 12 - Results Survey – Part 1 – System security

5.3 Results part 2

I didn't receive a lot of answers from system users, but two of the responding companies were kind enough to ask their users to answer the questionnaire.

Both are well-known Norwegian companies and have between 100 and 1000 employees, but for confidentiality reasons their names will not be mentioned. The results from these questionnaires are show in table 13 and 14. Explanations to the values in "learning curve" and "ease of use" can be found in appendix B table 22, while "time usage" and "user's ranking" can be found in appendix B table 23 and 24.

System 12 (from table 12) uses a smart card/PIN combination for authentication, while system 3 uses username/password. 23 and 20 users answered the questionnaire respectively.

Authentication method	Score M-4	Learning curve	Ease of use	Score M-5	Time usage	User's ranking	Score M-6
Smart card/PIN	1	1	1	5	2	2	4
Smart card/PIN	1	4	2	3	2	3	3
Smart card/PIN	1	2	2	4	2	2	4
Smart card/PIN	1	3	1	4	2	2	4
Smart card/PIN	1	2	2	4	3	1	5
Smart card/PIN	1	2	2	4	3	1	5
Smart card/PIN	1	1	1	5	2	2	4
Smart card/PIN	1	3	2	3,5	2	2	4
Smart card/PIN	1	3	2	3,5	3	3	3
Smart card/PIN	1	2	2	4	3	2	4
Smart card/PIN	1	2	2	4	2	2	4
Smart card/PIN	1	3	2	3,5	2	1	5
Smart card/PIN	1	1	1	5	2	1	5
Smart card/PIN	1	3	3	3	2	2	4
Smart card/PIN	1	2	1	4,5	2	2	4
Smart card/PIN	1	2	2	4	3	2	4
Smart card/PIN	1	3	3	3	3	3	3
Smart card/PIN	1	3	2	3,5	2	2	4
Smart card/PIN	1	1	1	5	2	2	4
Smart card/PIN	1	2	2	4	2	1	5
Smart card/PIN	1	2	2	4	3	2	4
Smart card/PIN	1	1	1	5	3	1	5
Smart card/PIN	1	3	2	3,5	2	2	4
AVERAGE	**1**			**4.00**			**4.13**

Table 13 - Results system 12 - M-4, M-5 and M-6

Authentication method	Score M-4	Learning curve	Ease of use	Score M-5	Time usage	User's ranking	Score M-6
PIN/Password	1	2	2	4	2	1	5
PIN/Password	1	3	3	3	3	2	4
PIN/Password	1	2	2	4	2	2	4
PIN/Password	1	2	2	4	2	2	4
PIN/Password	1	3	3	3	1	1	5
PIN/Password	1	3	2	3,5	2	2	4
PIN/Password	1	2	3	3,5	1	2	4
PIN/Password	1	2	2	4	1	2	4
PIN/Password	1	2	3	3,5	2	1	5
PIN/Password	1	1	2	4,5	2	3	3
PIN/Password	1	1	1	5	2	2	4
PIN/Password	1	3	2	3,5	2	2	4
PIN/Password	1	2	2	4	1	1	5
PIN/Password	1	1	1	5	2	2	4
PIN/Password	1	1	3	4	2	1	5
PIN/Password	1	2	3	3,5	2	1	5
PIN/Password	1	3	4	2,5	3	2	4
PIN/Password	1	3	2	3,5	2	3	3
PIN/Password	1	2	2	3,5	2	2	4
PIN/Password	1	2	2	4	1	1	5
AVERAGE	**1**			**3,775**			**4,25**

Table 14 - Results system 3 - M-4, M-5 and M-6

The following are the complete results for the two example systems, when used with the proposed methodology:

System 3:

Security: $d = \sqrt{(5-1)^2 + (5-3{,}5)^2 + (5-2)^2} = 5.22$

User-friendliness: $d = \sqrt{(5-1)^2 + (5-3{,}775)^2 + (5-4{,}25)^2} = 4.25$

System 12:

Security: $d = \sqrt{(5-3)^2 + (5-2{,}5)^2 + (5-4)^2} = 3.35$

User-friendliness: $d = \sqrt{(5-1)^2 + (5-4)^2 + (5-4{,}15)^2} = 4.21$

As can be seen from the calculations above system 12 receives a slightly better result than system 3 in the user-friendliness category, but gets an appreciably better score for security.

The figure below is an example on how the metrics can be represented in a three dimensional room and shows the position of systems 12 and 3 for the security metrics. I is the ideal point in (5x, 5y, 5z). As seen above, their scores are respectively 3.35 and 5.22 which is the distance from I.

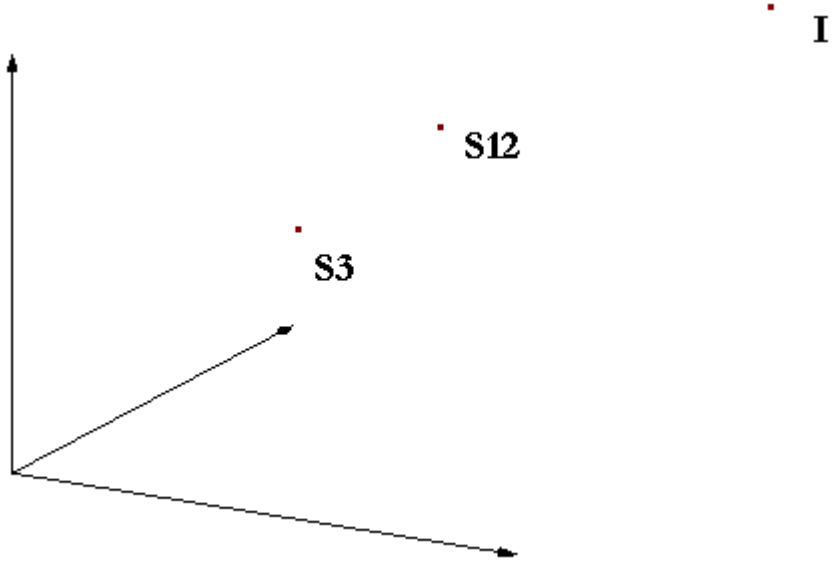


Figure 4 - Results for systems 3 and 12 in a three dimensional space

6 CONCLUSION

The proposed metrics in this thesis should enable companies, and others, to evaluate different authentication systems in respect of security and user-friendliness. They should also be a helpful tool for security managers to discern the effectiveness of various security components for both categories presented in chapter 3. They can also be used by security employers to demonstrate the effect of various security measures to management. By presenting the results as the distance between vectors in a three-dimensional space, we hope to ease how to interpret the results graphically, complementing the numerical results. It is important to note that the metrics only contain our chosen indicators and not a complete overview of security or user-friendliness.

As can be seen in figure 3 there is a predominance of companies using something one knows as the single chosen authentication method. These results coincide with the results from the CSI/FBI Computer crime and security survey (2007) [45], which is a report based on survey results of 494 computer security practitioners in U.S. corporations, government agencies, financial institutions, medical institutions and universities. Nine out of 17 companies (53 %) in our survey use static account log-in/password technique, while the number is 51 percent in the CSI-survey. This is a concerning fact as this authentication method alone is widely considered inadequate and contributes to making systems less secure.

7 of 17 (41.2%) companies in our survey use a more secure method of combination between at least 2 methods for authentication. Two companies (11.8%) use a combination of all three methods; something one knows, something one has and something one is, which is considered most secure.

17 out of all large scale Norwegian companies is a rather small selection so the results can probably not be generalized to the entire population, it should however provide some valid indicators. The selection in our survey was companies in ISF, which could also influence the results. These members are probably already concerned with security and could generate better results, with regards to security, than what would otherwise be the case. Another fact that might influence our result is that often only respondents with a general interest in the subject will answer an optimal questionnaire like this. It could also be that some simply does not understand the questions, thus not responding.

Even though the CSI Computer Crime Survey is related to US companies instead of Norwegian as in this thesis, we see some correlations to our survey that may prove its validity.

According to our survey users of username/password authentication and users of smart card/PIN authentication are reasonably satisfied with the ease of use and learning curve of their systems, but there seems to be even more satisfactory predominance among smart

card/PIN users. This could be related to difficulties concerning policies for password complexity and password retention.

Both example companies for part two of the survey are also members of ISF. They do most likely have an internal information security education program, which in turn could affect how the users respond to the questionnaire. They will probably have a better understanding for security and understand that security measures often create user-friendliness issues. Results could therefore be less positive within companies with the same authentication mechanisms, but where users don't have the same level of information security awareness.

FURTHER WORK

A list of secure/insecure algorithms should be created for Metric 2, Client server communication – cryptographic encryption and authentication quality. The indicators and formula should be revised to take weak contra strong algorithms into consideration. This will improve the overall quality of the metric. It should also be possible to award systems that use public key infrastructure [46] for added security.

Each metric could also be expanded with more indicators, but it is widely regarded as advisable to limit the number of indicators used. One could also differentiate some of the metrics based on type of authentication system identified in metric one, in such a way that the indicators become more specific for each technique. This would however make it impossible to evaluate two systems with different authentication techniques against each other.

In some cases it might be desirable to weigh the two categories, security and user-friendliness, so that the two vectors can be combined into a common domain. Possible solutions to this could include weighing the result from each category with a percentage ratio, or combining all 6 metrics in the same room. The latter would prevent a three dimensional representation, but Euclidean distance could still be used to measure distance to the ideal.

References:

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

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

[3] Lecture notes – Security metrics - Gjøvik University College 2004, Einar Snekkenes.

[4] John W. Creswell, "Research and Design - Qualitative, Quantitative and Mixed Methods Approaches", Sage Publications, ISBN 0-7619-2442-6.

[5] Andrew Odlyzko, "Economics, Psychology and Sociology of Security", Digital Technology Center., University of Minnesota,
http://www.dtc.umn.edu/~odlyzko/doc/econ.psych.security.pdf.

[6] Bruce Schneier, "Beyond fear - Thinking sensibly about security in an uncertain world", Copernicus Books 2003, ISBN 0-387-02620-7

[7] Matt Bishop, "Computer security – Art and Science", Addison-Wesley 2003, ISBN 0-201-44099-7.

[8] Richard E. Smith. From Passwords to Public Keys. Addison-Wesley. ISBN 0-201-61599-1.

[9] Want, R., An introduction to RFID technology, Pervasive Computing, IEEE, Volume 5, Issue 1, 2006.

[10] Tom Fladsrud and Roar S. Sollie. "Circumvention of fingerprint scanners" December 15, 2004. http://roarsollie.net/skole/Circumvention%20of%20fingerprint%20scanners%20-%20Autentisering.pdf.

[11] Roar Sollie, "Security and usability assessment of several authentication technologies", master's thesis – Master of Science in information security, Gjøvik University College. 2005.

[12] D. Maltoni, D. Maio, A. K. Jain and S. Prabhakar, "Handbook of Fingerprint Recognition", New York, 2003, Springer, ISBN 978-0387954318.

[13] 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.

[14] Torkjel Søndrol, "Using the human gait for authentication", master's thesis 2005, Gjøvik University College.

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

[16] Marijana Kosmerlj, "Passport of the Future: Biometrics against Identity Theft?", master's thesis 2004, Gjøvik University College.

[17] Marilyn Chun, "Authentication methods, which is best?", 2001, http://www.giac.org/certified_professionals/practicals/gsec/0594.php.

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

[19] Marianne Swanson, Nadya Bartol, John Sabato and Joan Hash, NIST 800-55, "Security Metrics Guide for Information Technology Systems", Technical Report NIST Special Publication, 2003, http://csrc.nist.gov/publications/nistpubs/800-55/sp800-55.pdf.

[20] Rayford B. Vaughn, Jr., Ronda Henning, Ambareen Siraj, "Information Assurance Measures and Metrics - State of Practice and Proposed Taxonomy", ISBN: 0-7695-1874-5.

[21] John M. Hugh, "Quantitative Measures of Assurance: Prophecy, Process or Pipedream?" CERT/CC, Software Engineering Institute, Carnegie Mellon University.

[22] Vaughn, R., Henning, R., Siraj, A. No date, " Information Assurance Measures and Metrics - State of Practice and Proposed Taxonomy", In Proceedings of the 36th Annual Hawaii International Conference on System Sciences (HICSS'03) - Track 9 - Volume 9. 2003, IEEE Computer Society.

[23] Bob Frost, "Measuring performance - Using new metrics to deploy strategy and improve performance", Measurement International, ISBN 0-9702741-1-7.

[24] Payne S. 2001, "A guide to security metrics", SANS Security Essentials GSEC Practical assignment (Revisited June 2006), http://www.sans.org/rr/papers/5/55.pdf.

[25] Edward G. Carmines and Richard A. Zeller, "Reliability and validity assessment", Sage Publications, 1976, ISBN 0803913710.

[26] Christian Gehrmann and Mats Naslund (ERICS), "ECRYPTY - Early Report on Algorithms and Key sizes", European Network of Excellence in Cryptology (2006).

[27] Elaine Barker, William Barker, William Burr, William Polk, and Miles Smid, "Recommendation for Key Management – Part 1: General (Revised)", NIST Special Publication 800-57, March, 2007.

[28] William C. Barker, Special Publication 800-67, "Recommendation for Triple Data Encryption Algorithm Block Cipher", May 2004.

[29] Federal Information Processing Standard 197, Advanced Encryption Standard (AES), November 2001.

[30] Morris Dworkin, NIST Special Publication 800-38B, "Recommendation for Block Cipher Modes of Operation: The RMAC Authentication Mode".

[31] Federal Information Processing Standard 186-3, "Digital Signature Standard (DSS)", (Revision of FIPS 186-2, June 2000).

[32] PKCS #1 v2.1, "RSA Cryptography Standard", RSA Laboratories, June 14, 2002.

[33] Elaine Barker, Don Johnson, and Miles Smid. Special Publication 800-56, "Recommendation on Key Establishment Schemes".

[34] Arjen K. Lenstra, "Key Lengths - Contribution to The Handbook of Information Security" (revised version, June 30, 2004).

[35] Arjen K. Lenstra, Eric R.Verheul, "Selecting Cryptographic Key Sizes", Journal of Cryptology: the journal of International Association for Cryptographic Research, 14(4):255-293, 2001.

[36] Douglas R. Stinson, "Cryptography – Theory and practice second edition", Chapman & Hall/CRC, ISBN 1-58488-206-9

[37] "ITSEC, information technology security evaluation criteria", Harmonized Criteria of France, Germany, the Netherlands and the United Kingdom.

[38] Common Criteria for information technology and security evaluation, ISO/IEC 15408.

[39] International ISO/IEC STANDARD 17799, "Information technology — Code of practice for information security management".

[40] ISO 9126 (1991) Software Engineering Product Quality, "International standard for the evaluation of software".

[41] ISO 9241, "Ergonomic requirements for office work with visual display terminals", Part 11: Guidance on usability.

[42] Henning Gravnås, "Users trust in biometric authentication systems", Master's thesis, Gjøvik University College, 2005.

[43] 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.

[44] IT-sikkerhetsforum, www.isf.no.

[45] Robert Richardson, CSI – Computer Crime and Security Survey, Computer Security Institute, http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf

[46] Jianying Zhou, "Non-repudiation in Electronic Commerce", Artech House, ISBN 1-58053-247-0.

Appendix A - Questionnaire

This Questionnaire has been created to discover the level of security and user-friendliness in large scale Norwegian companies.

Part 1 – for system administrators or system owners.

M 1 - Authentication method.

1. What kind of authentication method does the system use? If the system requires a combination of several alternatives please check for each method, e.g. one-time passwords (OTP), in combination with a secret:

- No authentication
  Yes ☐ No ☐

- Pin/Password, something you know
  Yes ☐ No ☐

- Smartcard, something you have
  Yes ☐ No ☐

- OTP, something you have
  Yes ☐ No ☐

- Biometric authentication, something you are
  Yes ☐ No ☐
  Please specify type of biometry (e.g. fingerprints, iris, retina, face recognition etc.) [ ]

- Other
  Yes ☐ No ☐

  Description [ ]

M 2 – Client Server Communication – encryption and authentication quality

2. Is the client-server communication properly secured using encryption and authentication algorithms?

- Encryption in client – server connection
  Yes ☐ No ☐

- Authentication in client – server connection
  Yes ☐ No ☐

If implemented:

- Type of encryption algorithm:
  [ ]
  - Size of key:
  [ ]

- Type of authentication algorithm:
  [ ]
  - Size of key:
  [ ]

M 3 – Secure log-on associated procedures

3. Is the log on procedure associated with the authentication secured with the following techniques?

- If error condition arises, the system does not indicate which part of the data is correct or un-correct.
  Yes ☐ No ☐

- Limit number of unsuccessful logon attempts with one or more of the following consequences; time delay until next possible authentication attempt, recording unsuccessful attempts, disconnect connection, alarm trap:
  Yes ☐ No ☐

- Limit the maximum allowed log-on time:
  Yes ☐ No ☐

- Does the system display the following information on completion of successful authentication attempts:
  Date and time of last successful authentication and detail on any unsuccessful attempts:
  Yes ☐ No ☐

- All users have their own unique identifier which is for personal use only:
  Yes ☐ No ☐

Part 2 – for system users.

Please fill in registration information:

Age: [ ]

Sex: Male ☐ Female ☐

M 4 - Authentication method – User friendliness.

4. What kind of authentication method does the system use?

- If the system requires a combination of several alternatives please check for each method:

  - No authentication
    Yes ☐ No ☐

  - Pin/Password, something you know
    Yes ☐ No ☐

  - Smartcard, something you have
    Yes ☐ No ☐

  - OTP, something you have
    Yes ☐ No ☐

  - Biometric authentication, something you are
    Yes ☐ No ☐
    Please specify type of biometry [ ]

  - Other
    Yes ☐ No ☐
    Description [ ]

M 5 - Authentication method – Ease of use.

5. Do you find the authentication phase of using the system easy to use?

- Please grade your opinion based on a scale of points where 2,5 is very easy and 0 is very difficult.
    - Initial learning curve:

      Easy 2,5 ☐ 2 ☐ 1,5 ☐ 1 ☐ 0,5 ☐ 0 ☐ Difficult

    - What is your opinion on how easy the authentication phase is to use?
      Please assume that the initial learning phase is over and consider the rate of errors (includes forgetting PIN or password):

      Easy 2,5 ☐ 2 ☐ 1,5 ☐ 1 ☐ 0,5 ☐ 0 ☐ Difficult

M 6 - Authentication method – Speed of performance.

6. What is your opinion on how long it takes to authenticate using?

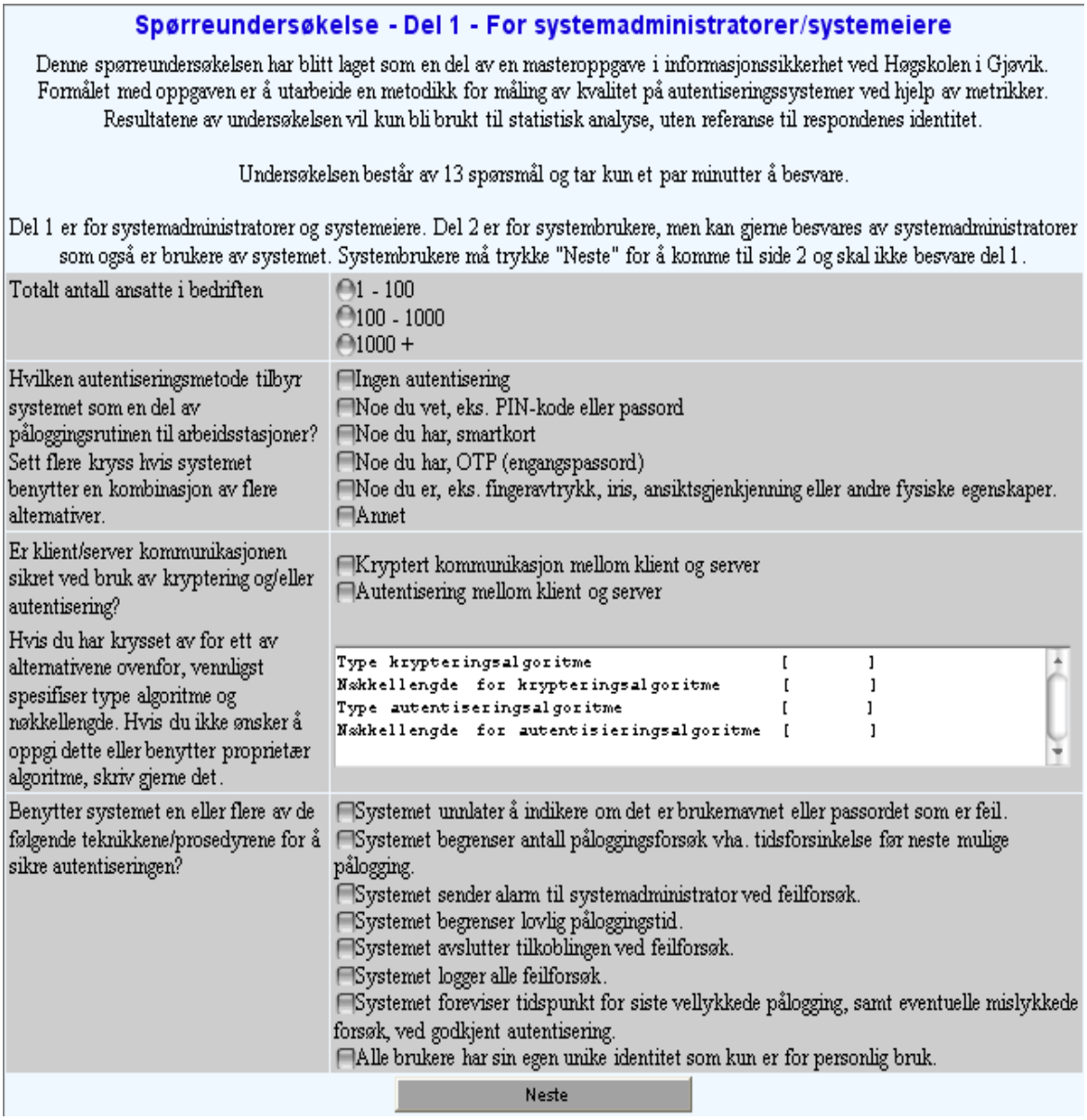
- Please grade your opinion based on a scale of points where 5 is very acceptable and 0 not acceptable at all. Please assume that the initial learning phase is over.
    - Your rating:

      Acceptable 5 ☐ 4 ☐ 3 ☐ 2 ☐ 1 ☐ 0 ☐ Not acceptable

    - How long does an average authentication take in seconds

      [_____ seconds]

Questionnaire - Web based version



Spørreundersøkelse - Del 1 - For systemadministratorer/systemeiere

Denne spørreundersøkelsen har blitt laget som en del av en masteroppgave i informasjonssikkerhet ved Høgskolen i Gjøvik. Formålet med oppgaven er å utarbeide en metodikk for måling av kvalitet på autentiseringssystemer ved hjelp av metrikker. Resultatene av undersøkelsen vil kun bli brukt til statistisk analyse, uten referanse til respondenes identitet.

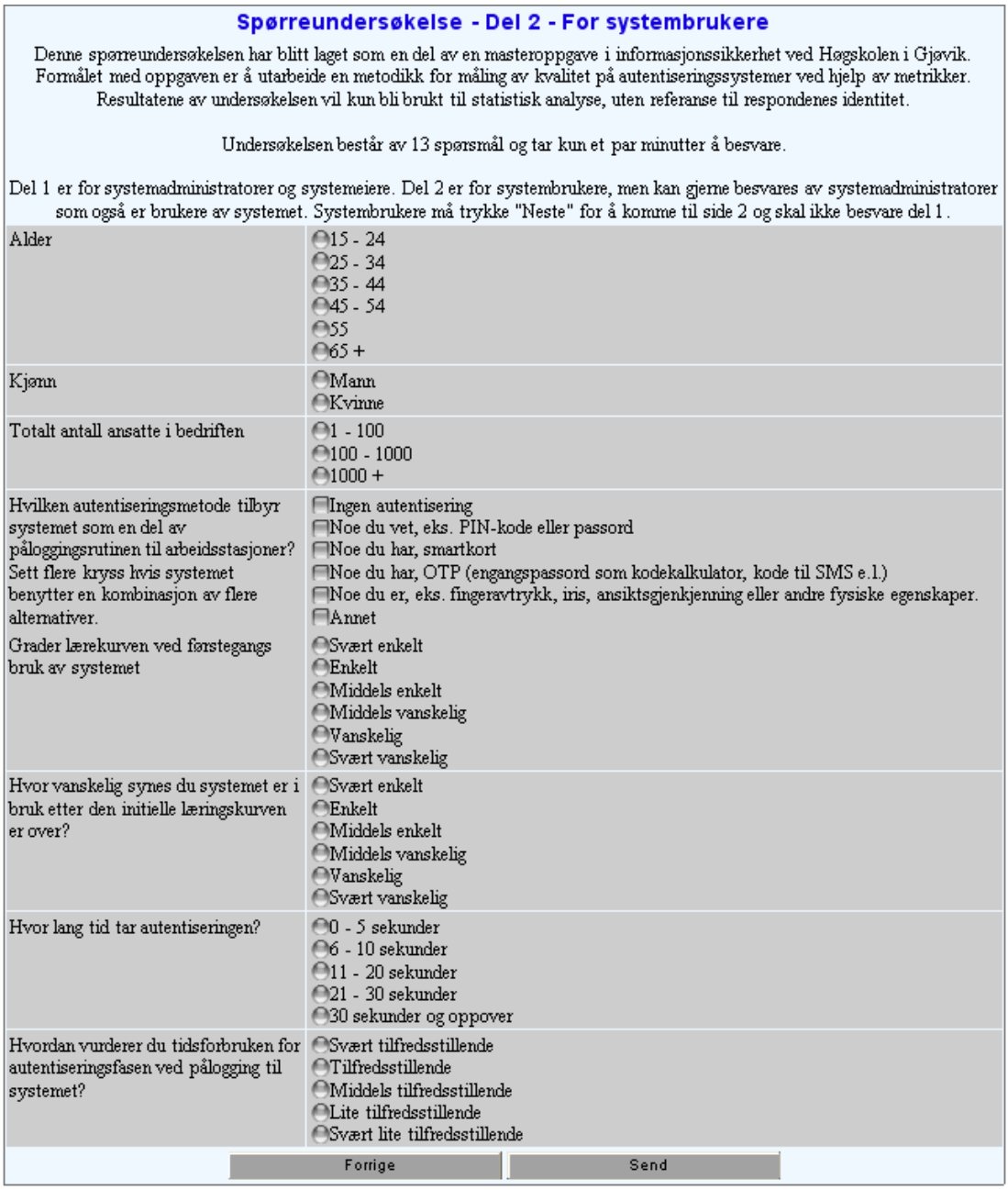
Undersøkelsen består av 13 spørsmål og tar kun et par minutter å besvare.

Del 1 er for systemadministratorer og systemeiere. Del 2 er for systembrukere, men kan gjerne besvares av systemadministratorer som også er brukere av systemet. Systembrukere må trykke "Neste" for å komme til side 2 og skal ikke besvare del 1.

Totalt antall ansatte i bedriften	○ 1 - 100 ○ 100 - 1000 ○ 1000 +
Hvilken autentiseringsmetode tilbyr systemet som en del av påloggingsrutinen til arbeidsstasjoner? Sett flere kryss hvis systemet benytter en kombinasjon av flere alternativer.	☐ Ingen autentisering ☐ Noe du vet, eks. PIN-kode eller passord ☐ Noe du har, smartkort ☐ Noe du har, OTP (engangspassord) ☐ Noe du er, eks. fingeravtrykk, iris, ansiktsgjenkjenning eller andre fysiske egenskaper. ☐ Annet
Er klient/server kommunikasjonen sikret ved bruk av kryptering og/eller autentisering?	☐ Kryptert kommunikasjon mellom klient og server ☐ Autentisering mellom klient og server
Hvis du har krysset av for ett av alternativene ovenfor, vennligst spesifiser type algoritme og nøkkellengde. Hvis du ikke ønsker å oppgi dette eller benytter proprietær algoritme, skriv gjerne det.	Type krypteringsalgoritme [ ] Nøkkellengde for krypteringsalgoritme [ ] Type autentiseringsalgoritme [ ] Nøkkellengde for autentisieringsalgoritme [ ]
Benytter systemet en eller flere av de følgende teknikkene/prosedyrene for å sikre autentiseringen?	☐ Systemet unnlater å indikere om det er brukernavnet eller passordet som er feil. ☐ Systemet begrenser antall påloggingsforsøk vha. tidsforsinkelse før neste mulige pålogging. ☐ Systemet sender alarm til systemadministrator ved feilforsøk. ☐ Systemet begrenser lovlig påloggingstid. ☐ Systemet avslutter tilkoblingen ved feilforsøk. ☐ Systemet logger alle feilforsøk. ☐ Systemet foreviser tidspunkt for siste vellykkede pålogging, samt eventuelle mislykkede forsøk, ved godkjent autentisering. ☐ Alle brukere har sin egen unike identitet som kun er for personlig bruk.

Neste

Figure 5 - Questionnaire - web version - Part 1



Spørreundersøkelse - Del 2 - For systembrukere

Denne spørreundersøkelsen har blitt laget som en del av en masteroppgave i informasjonssikkerhet ved Høgskolen i Gjøvik. Formålet med oppgaven er å utarbeide en metodikk for måling av kvalitet på autentiseringssystemer ved hjelp av metrikker. Resultatene av undersøkelsen vil kun bli brukt til statistisk analyse, uten referanse til respondenes identitet.

Undersøkelsen består av 13 spørsmål og tar kun et par minutter å besvare.

Del 1 er for systemadministratorer og systemeiere. Del 2 er for systembrukere, men kan gjerne besvares av systemadministratorer som også er brukere av systemet. Systembrukere må trykke "Neste" for å komme til side 2 og skal ikke besvare del 1.

Alder	○ 15 - 24 ○ 25 - 34 ○ 35 - 44 ○ 45 - 54 ○ 55 ○ 65 +
Kjønn	○ Mann ○ Kvinne
Totalt antall ansatte i bedriften	○ 1 - 100 ○ 100 - 1000 ○ 1000 +
Hvilken autentiseringsmetode tilbyr systemet som en del av påloggingsrutinen til arbeidsstasjoner? Sett flere kryss hvis systemet benytter en kombinasjon av flere alternativer.	☐ Ingen autentisering ☐ Noe du vet, eks. PIN-kode eller passord ☐ Noe du har, smartkort ☐ Noe du har, OTP (engangspassord som kodekalkulator, kode til SMS e.l.) ☐ Noe du er, eks. fingeravtrykk, iris, ansiktsgjenkjenning eller andre fysiske egenskaper. ☐ Annet
Grader lærekurven ved førstegangs bruk av systemet	○ Svært enkelt ○ Enkelt ○ Middels enkelt ○ Middels vanskelig ○ Vanskelig ○ Svært vanskelig
Hvor vanskelig synes du systemet er i bruk etter den initielle læringskurven er over?	○ Svært enkelt ○ Enkelt ○ Middels enkelt ○ Middels vanskelig ○ Vanskelig ○ Svært vanskelig
Hvor lang tid tar autentiseringen?	○ 0 - 5 sekunder ○ 6 - 10 sekunder ○ 11 - 20 sekunder ○ 21 - 30 sekunder ○ 30 sekunder og oppover
Hvordan vurderer du tidsforbruken for autentiseringsfasen ved pålogging til systemet?	○ Svært tilfredsstillende ○ Tilfredsstillende ○ Middels tilfredsstillende ○ Lite tilfredsstillende ○ Svært lite tilfredsstillende

Forrige | Send

Figure 6 - Questionnaire - web version - Part 2

Appendix B - Questionnaire – Results

System nr.	Number of employees	Authentication method	Score M-1
1	100 - 1000	Combination of 2 and 3	3.0
2	100 - 1000	Combination of 2, 4 and 5	5.0
3	100 - 1000	2	1.0
4	1000+	Combination of 2, 3 and 5	5.0
5	1000+	2	1.0
6	1000+	2	1.0
7	1000+	2	1.0
8	1000+	2	1.0
9	100 - 1000	1	0.0
10	100 - 1000	2	1.0
11	100 - 1000	2	1.0
12	100 - 1000	Combination of 2 and 3	3.0
13	100 - 1000	2	1.0
14	100 - 1000	2	1.0
15	100 - 1000	Combination of 2 and 4	3.0
16	100 - 1000	Combination of 2 and 3	3.0
17	1000+	Combination of 3 and5	4.0

Table 15 - Results questionnaire M-1

Authentication method	Representing value
No authentication	1
Something one knows, PIN/password	2
Something one has, smart card	3
Something one has, OTP	4
Something one is, biometrics	5
Other	6

Table 16 - Authentication method - representing value

System nr.	Encryption	Authentication	Encryption alg.	Key length	Authentication algorithm	Key length	Score	Score key length	Score M-2
1	Yes	No	AES	256			1.0	1.5	2.5
2	Yes	No	AES	512			1.0	1.5	2.5
3	Yes	Yes	AES	256	No answer	No answer	2.0	1.5	3.5
4	Yes	Yes	AES	256	Digital sertificates	1024	2.0	3.0	5.0
5	Yes	Yes	No answer	No answer	No answer	No answer	2.0	0.0	2.0
6	No	No					0.0	0.0	0.0
7	No	No					0.0	0.0	0.0
8	Yes	Yes	AD	AD	AD	AD	2.0	3.0	5.0
9	No	Yes			No answer	No answer	1.0	0.0	1.0
10	No	Yes			No answer	No answer	1.0	0.0	1.0
11	No	No					0.0	0.0	0.0
12	Yes	No	AES	256			1.0	1.5	2.5
13	No	No					0.0	0.0	0.0
14	Yes	No	AES	256			1.0	1.5	2.5
15	Yes	Yes	DES	256		512	2.0	3.0	5.0
16	Yes	No	AES	256			1.0	1.5	2.5
17	Yes	Yes	AES	256			2.0	1.5	3.5

Table 17 - Results questionnaire M-2

System nr.	Implemented procedures	Score M-3
1	2, 3, 6 and 8	2.0
2	2, 3, 6, 7 and 8	3.0
3	2, 3, 6 and 8	2.0
4	1, 3, 5, 7 and 8	4.0
5	1, 2, 6 and 8	3.0
6	1, 2, 3, 8	3.0
7	1, 5, 7 and 8	4.0
8	1, 3, 6 and 8	3.0
9	3 and 6	1.0
10	1, 2, 4, 6, 7 and 8	5.0
11	1, 2, 6 and 8	3.0
12	1, 2, 3, 6, 7 and 8	4.0
13	1, 2, 6 and 8	3.0
14	1, 2, 6, 7 and 8	4.0
15	7 and 8	2.0
16	1, 6 and 8	3.0
17	1, 7 and 8	3.0

Table 18 - Results questionnaire M-3

Procedure	Representing value
The system does not indicate which part of the data is correct or un-correct	1
Limit number of unsuccessful logon attempts with time delay until next attempt	2
Alarm trap to system administrator after unsuccessful attempts	3
Disconnect after unsuccessfull attempt	4
Logging of all log-on errors	5
Limit the maximum allowed log-on time	6
Display date and time of last successful authentication and detail on any unsuccessful attempts, after successful log-on attempts	7
All users have their own unique identifier which is for personal use only	8

Table 19 - Procedure - representing value

Authentication method	Score M-4	Learning curve	Ease of use	Score M-5	Time useage	User's ranking	Score M-6
Smart card + PIN	1.0	1	1	5.0	2	2	4.0
Smart card + PIN	1.0	4	2	3.0	2	3	3.0
Smart card + PIN	1.0	2	2	4.0	2	2	4.0
Smart card + PIN	1.0	3	1	4.0	2	2	4.0
Smart card + PIN	1.0	2	2	4.0	3	1	5.0
Smart card + PIN	1.0	2	2	4.0	3	1	5.0
Smart card + PIN	1.0	1	1	5.0	2	2	4.0
Smart card + PIN	1.0	3	2	3.5	2	2	4.0
Smart card + PIN	1.0	3	2	3.5	3	3	3.0
Smart card + PIN	1.0	2	2	4.0	3	2	4.0
Smart card + PIN	1.0	2	2	4.0	2	2	4.0
Smart card + PIN	1.0	3	2	3.5	2	1	5.0
Smart card + PIN	1.0	1	1	5.0	2	1	5.0
Smart card + PIN	1.0	3	3	3.0	2	2	4.0
Smart card + PIN	1.0	2	1	4.5	2	2	4.0
Smart card + PIN	1.0	2	2	4.0	3	2	4.0
Smart card + PIN	1.0	3	3	3.0	3	3	3.0
Smart card + PIN	1.0	3	2	3.5	2	2	4.0
Smart card + PIN	1.0	1	1	5.0	2	2	4.0
Smart card + PIN	1.0	2	2	4.0	2	1	5.0
Smart card + PIN	1.0	2	2	4.0	3	2	4.0
Smart card + PIN	1.0	1	1	5.0	3	1	5.0
Smart card + PIN	1.0	3	2	3.5	2	2	4.0

Table 20 - Results from company 1 – Combination of smart card and PIN

Authentication method	Score M-4	Learning curve	Ease of use	Score M-5	Time useage	User's ranking	Score M-6
Username/Password	1.0	2	2	4.0	2	1	5.0
2	1.0	3	3	3.0	3	2	4.0
2	1.0	2	2	4.0	2	2	4.0
2	1.0	2	2	4.0	2	2	4.0
2	1.0	3	3	3.0	1	1	5.0
2	1.0	3	2	3.5	2	2	4.0
2	1.0	2	3	3.5	1	2	4.0
2	1.0	2	2	4.0	1	2	4.0
2	1.0	2	3	3.5	2	1	5.0
2	1.0	1	2	4.5	2	3	3.0
2	1.0	1	1	5.0	2	2	4.0
2	1.0	3	2	3.5	2	2	4.0
2	1.0	2	2	4.0	1	1	5.0
2	1.0	1	1	5.0	2	2	4.0
2	1.0	1	3	4.0	2	1	5.0
2	1.0	2	3	3.5	2	1	5.0
2	1.0	3	4	2.5	3	2	4.0
2	1.0	3	2	3.5	2	3	3.0
2	1.0	2	2	3.5	2	2	4.0
2	1.0	2	2	4.0	1	1	5.0

Table 21 - Results from company 2 – Username/password

Alternative	Value	Metric score
Very easy	1	2,5
Easy	2	2,0
Medium easy	3	1,5
Medium difficult	4	1,0
Difficult	5	0,5
Very difficult	6	0,0

Table 22 - Explanation to the values of learning curve and ease of use

Time in seconds	Value
0 - 5	1
6 - 10	2
11 - 20	3
21 - 30	4
30 +	5

Table 23 - Explanation to the time in seconds value

User's ranking	Value	Metric score
Very satisfactory	1	5,0
Satisfactory	2	4,0
Medium satisfactory	3	3,0
Less satisfactory	4	2,0
Very unsatisfactory	5	1,0

Table 24 - Explanation to the user's ranking value