INTERNATIONELLA HANDELSHÖGSKOLAN
HÖGSKOLAN I JÖNKÖPING

Inloggningssystem för internet banker

Principer och val av bakomliggande faktorer och framtida utveckling, sett ur ett ledningsperspektiv

Filosofie kandidat inom informatik

Författare: Patrik Ekberg
Sofia Li
Gentiana Morina

Handledare: Jörgen Lindh

Framläggningsdatum 070601

Jönköping juni 2007

JÖNKÖPING INTERNATIONAL BUSINESS SCHOOL
Jönköping University

Online banking access system

Principles behind choices and further development, seen from a managerial perspective

Bachelor's thesis within informatics

Author: Patrik Ekberg
Sofia Li
Gentiana Morina

Tutor: Jörgen Lindh

Jönköping June 2007

Bachelor'sThesis in Informatics

Title: **Online banking access system: Principles behind choices and further development**

Author: **Patrik Ekberg**

Sofia Li

Gentiana Morina

Tutor: **Jörgen Lindh**

Date: **2007-06-01**

Subject terms: **online banking, internet banking, ebanking, online banking access system**

Abstract

Online banking is a young way for banks to reach new and old customers. The concept has emerged over the last decade from being not very utilized to become a major channel for the bigger banks in Sweden but also in the world. This thesis will present a study of what principles the four major Swedish banks have based their decision on when choosing what type of online access system to use. Furthermore try to present what the future principles might be toward online banking access systems. This might also show how new systems might look like and what the banks strives to achieve when making these systems not only safer but more available and usable. The thesis will present what authentication is and how the authentication process is used today. Today in general what is used is the two factor authentication which is based upon passwords. This two factor authentication makes it hard for attackers to breach the systems in use today, but there are ways which are emerging to gain access. Such an emerging threat is the SSL-evading Trojans. Still these kinds of threats are not common at all but they need to be considered. Today passwords are the only means we can use to make the authentication processes safe but they are not enough, according to Bill Gates. Therefore we have looked at new ways to complement today's password based authentication processes; such compliments might be the use of biometrics, which seems to be an emerging technology.

This study have been a challenge from the beginning since we knew that this is a very intense subject for the banks to discuss and therefore we have had to be persuasive in many cases and let the banks answer anonymously to be able to gather as much information as possible from our sample banks. Furthermore we have collected up to date articles and studies to be able to get as accurate information as possible.

The main findings we have discovered is the trade-off between security versus availability and flexibility and these factors were the same no matter what online access system, PDA or smart card, they have in use. But also that all the banks states that their authentication process is very safe and striving to become 100% secure, even though we have found new threats which is not of an authentication problem but a matter of transactional problem. The banks have shown through the interviews that they lack awareness of such a threat.

Table of Contents

Figure

Appendices

1 Introduction

In this chapter we will start by introduce how we look upon the phenomena of online banking and online banking access systems in use today and why this is interesting. Furthermore we will present the purpose with the study and who we believe will have an interest in the matter. Last we will present some definitions.

1.1 Background

As we see it in today's society there is a change in the life cycle process between growth and maturity. A factor that affects our society is the high developing technology, which both individuals and companies can gain major benefits from what the technology provides.

The information technology (IT) with its complex systems provides different organisations with numerous advantages, but this in turn also leads to a lot of challenges concerning security issues. A more specific area is the financial institutions such as banks, where security have become a high essential matter. Because of the fact that the systems are exposed by different kind of threats, the security question must be an on-going process during the development process. This requires from the bank to have both the skill and knowledge and provide high a security support for their customers as a part of the service.

Today banks can offer their customers the service of online banking, which is an opportunity for the customer to quickly and efficiently in anytime, handle their private banking routines from any computer with a few clicks. The evolvement of online banking have developed from, customers going to their local bank and handling their banking commissions and transactions, to handle these transactions online instead. Since banks handle very sensitive information, such as people's and companies' finances, this has lead to the rising issues of online banking security. To meet the high level of security expected from banks online services, banks have taken several undertakings such as using Socket secure layer (SSL), see definitions, offer antivirus and firewall protections through their own websites and also better authentication processes (Hines. 2006). This means that more and more banks are starting to use two factor authenticating processes, explained in the theoretical framework, to make it harder to crack passwords and gain unauthorized access. Today online banking is a prioritized issue for every bank in order to retain existing customers.

Furthermore, different banks offer different solutions of online banking with different options for their customers to simplify everyday life. In more detail, the different online banking has different ways of security access to personal accounts. From the customers' perspective, this can affect their choice of bank based on the banks security level and their loyalty towards the bank.

1.2 Problemdiscussion

As stated before the changes from doing banking services in a brick and mortar bank to do them over internet instead, leads us to wonder about the different ways banks are letting their customers get access to their online bank. The banks offer different ways to guarantee the safety of this access. In Sweden there are mainly two different systems used, the one-time codes given on a card sent to the customer, which is used together with the specific user's authorization, username and another password. The other system which banks in Sweden are using is the PDA system, every customer gets a specific PDA connected to their personnel number, and then by typing in some given codes on the webpage the cus-

tomer gets a unique new password from the PDA every time they log in to the personal online bank account. This will be further discussed in the theoretical framework mainly under the two-factor authentication.

When reading different articles and more in depth studies about the subject which we refer to as online banking, which also can be called e-banking or internet banking, we find that European western world is leading when it comes to security regarding the authentication processes. This leads us to the questions of how well is Sweden as a nation when it comes to this type of security and moreover what type of systems are being used and prioritized in Sweden. Further, are there any differences between the systems used today by Swedish banks?

Our research will be focused on what principles are behind the decisions of online banking access systems. This will hopefully show tendencies of decisions both now and what principals might be dominating in the future. In the near future we mean within two to five years. Will there be one single dominating system, for example will banks focus on a specific system like biometric systems, fingerprint recognition, to reach maximum security or will it stay more like it is today? Hence too much security might end up with to high complexity; there is always a tradeoff between the confidentiality, the integrity and the availability (Bishop. 2005).

In more detail, our research questions will therefore be:

- What are the principles which the banks rely on in their decisions regarding online banking access systems?
- What principles will the banks have to take into account in their online access systems in the near future? (two to five years)

1.3 Purpose

The purpose with our study is to understand the principles behind the decisions made of the online banking access systems in use by the banks today, and try to conclude what might become the dominating principles behind the decisions in the future. Hence what type of systems will be used?

1.4 Perspective statement

A perspective statement is necessary for the internal use, and it is a process of analyzing and developing different hypothesis and understandings about what involves the research area (Goldkuhl. 1998). From our perspective of online banking, we know that different banks in Sweden offer different online banking access systems. We want to know the principles behind the decisions when choosing online banking access system in Sweden.

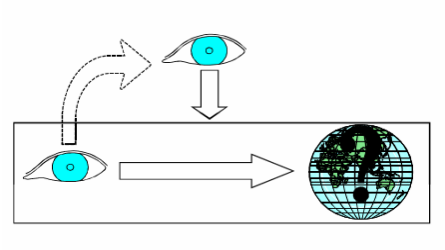

Figure 1 To see the entity from internal perspective (Goldkuhl, 1998 p.14)

According to Goldkuhl (1998) first you look upon a phenomenon from a normal perspective and then analyze that perspective to come up with a problem statement about that phenomenon, in this case online banking access systems. This will become our perspective. As stated in the background and problem discussion which is how we look upon online banking, is displayed by the upper eye in the figure, hence our perspective or perspective analysis of the phenomena of online banking and online banking access systems. A perspective is a way of looking upon the reality or world, meaning basic assumptions and which often are unreflected and implicit thoughts about the phenomena. This is displayed in figure one by the lower eye inside the box (Goldkuhl. 1998).

As discussed about problem and purpose, this study will be researched related to a managerial point of view, hence when banks decide which system to use; we assume they try to give their customers the best solution available. It is not the users that choose the actual access system that is offered. If the online banking system would be seen from a customer point of view then it would be a matter of an interaction between the computer and the customer or evaluating the interface. Therefore our perspective statement is a managerial choice, which leads our research questions to be seen in a managerial point of view.

Our implication of our thesis will hopefully show other perspectives for managers when analyzing today's online banking system. Furthermore, after analyzing the systems, it will hopefully create a guideline for the managers in the coming future of online banking.

We also have to set the limit of not putting focus on the end-user and the interaction with the online banking system, since it is not our main concern for this thesis to evaluate how the end-customer interacts with a computer.

1.5 Delimitation

First of all we decide to delimit our research area to a managerial point of view, the next step was to delimit the study to a national matter and finally we have to focus on the banks that offer this online banking service to their customers. This in order to find out what principles the different systems use today and what lies behind the decisions made by the bank. This will be a help for us in order to compare these systems and evaluate what would be the most suitable system in the near (two to five years) future.

All the information found regarding the subject of online banking is mostly concerning online banking as a general subject world wide and not specified as a subject seen from a specific countries point of view. Furthermore, the articles and more in depth studies found is mostly talking about online banking authentication as a common security issue world wide and therefore is it hard to find information regarding the systems in use from Swedish banks. Some information, studies and different examples from other specific countries do exist but not to any meaningful extent. Hence, we will not write about the differences that may, very likely, exist between countries.

1.6 Stakeholders

The stakeholders of our study consist of those individuals who use online banking today, and those who are considering applying to this online banking service that is offered from the different banks, and especially the banks themselves are important stakeholders to take into consideration. The customers as stated above might be interested in this report because they may feel more reluctant to use the service when knowing more about the systems in use and how they work in a general way. Thus the banks might have the biggest interests since this study hopefully will present some new findings which they lack awareness of and by doing that increase it and hopefully lead to safer and better authentication systems in a near future or in the future.

We believe that this study will create a more general picture of how the security of online banking access systems is working today, and also by reading this study would moreover result in making the users aware of the emergent threats. Furthermore ideas about new ways to complement the authentication process of only use passwords by more accurate authentication procedures.

Like stated above the banks are also stakeholders since it would be in their interest to have knowledge about threats in order to reach the maximum security possible. For those stakeholders who wish to have a deeper knowledge of this subject can also find relevant data in this study.

1.7 Definition

Authentication = the link of an identify to a subject, where the user trying to prove its own identification. Passwords are the most basic authentication mechanism (Bishop. 2004).

Biometrics – studies within science and technology of measuring and analyzing biological data of human characteristics, such as fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements, this for authentication purposes (TeachTarget. 2007)

Online banking – This is the definition we will use when talking about transactions made internet with a bank.

Online bank access – When using this word in our thesis we refer to the different ways that banks use to let their customers gain access to their internet bank.

Password – information that is personal related to an individual, which also confirms the individul's identity (Bishop. 2004).

Phishing – sending an e-mail to a user pretending to be an reputable legimitate enterprise, in attempt to sting the user with private information that will be later used for identity theft (Internet.com 2007).

PDA – This stands for "Personal Digital Assistant", we use this word when referring to the device given to customers from various banks to obtain a specific code to gain access to their internet bank.

SSL – According to WDA.org (2007) SSL is defined and this is the definition we will refer to. **"**Secure Sockets Layer. Used by most commerce servers on the World Wide Web, this high-level security protocol protects the confidentiality and security of data while it is being transmitted through the internet. SSL is an open protocol that has been submitted to sev-

eral industry groups as the industry security standard. Denoted by the letters HTTPS in the URL"

Trojan – a threat, a program that seems to be legitimate, but executes illegal acitivity when it runs. It may be used to track password information or makes the system vulnerable in future entrance or basically destroy softwares or data on the hard disk (Pcmag. 2006).

2 Method

In this chapter we will present how we have conducted the study and what type of knowledge we believe we will be able to find from our research. We also present what type of method we have chosen and why.

2.1 Pre-comprehension

Through our study we will need to follow a method, in order to get a result. For that reason, we need to have a primary definition of what a method is. According to Andersen (1994) a method is an exact description of how to solve a certain problem. By using models and given directions, "Guidelines for Bachelor Theses in Informatics", for the development of the work.

In our case this consists of studying today's and future guidelines concerning online banking. A method for our study will be a helping tool in evaluating and helping us during our study. Furthermore the method we choose will in addition facilitate us during the gathering of our data, and analyzing phase, due to the fact that we will then know how to gather the needed data and also how to analyze the data in order to achieve our purpose.
Moreover there are a number of factors to take into consideration when thinking about the structure of our study. One such immense factor is that the information regarding the security is very sensitive information for banks to give out; another factor is the concern for how far we may go before interfering and more importantly trespassing on the law of personal integrity (PUL) and also the law of confidentiality. In more detail, PUL, which is a Swedish law and stands for "Personlighets lagen", where the purpose is to protect people against invasion of personal integrity (SFS. 1998).

Furthermore, there is a reason for why this law exists, the main purpose is to protect, and prevent possible damage that individuals can be exposed to when using online banking. Moreover we also have to take ethics in consideration regarding the sensitive information of our study.

As mention by Holme & Solvang (1996) respect is crucial when studying individuals' integrity, which will also be applied in our study. Furthermore, our study will discuss the principles behind the choices of online banking. In relation to the research area we have chosen we need to consider the sensitivity of the ethics involved because the security is a very sensitive issue for the banks, but also for their customers. To be able to fulfill our purpose in a good way we believe it is of a high interest that we take this perspective about ethics on an early stage.

2.1.1 Anonymous security

According to Ejvegård (1996) objectivity is hard to reach when writing a report. Moreover, it is one immense obligation authors have to strive towards when conducting studies. In additional to this Carlsson (1984) discusses in his book "Forskningsmetodik" about the great impact peoples' anonymity has on studies, if the participants wish to be anonymous then he should be offered anonymity. This in turn could be done by gathering the data needed and more importantly by protecting this data in question so that unauthorized people are unable to come in contact with that information (Carlsson. 1984). According to Ejvegård (1996) there is a demand in relation to the choice of words and terminology a researcher needs to consider.

Furthermore by differentiating the data gathered from the investigation entity, researchers can obtain the anonymous security. If the researcher needs to connect the gathered data with the investigation entity, then there are a number of measurements of caution that can be maintained in order to preserve anonymous security. These involve for instance the changing of a particular name that are used in the gathered data, to be substitute with code number that would be destroyed when they are no longer necessary, or that research findings would be presented as group mean value, where value could not be discerned (Carlsson. 1984).

Bell and Opie (2002) discusses the meaning and the importance of confidentiality and anonymity when conducting interviews. According to the authors they stated that confidentiality is recognized as a promise that one will not be identified or presented in an identifiable form, hence they also declared that anonymity is a guarantee that even the researcher have a responsibility to not tell which responses came from which respondent (Bell & Opie. 2002).

For our study this will have a great impact on our empirical findings in such a way that we have informed our sample banks of their choice of anonymity. This will be done through stating this in the pre-given material, our interview guidelines, given to the banks before conducting the interviews. Since our research area is a high sensitive concern for the sample banks, this has been a highly prioritized matter when conducting the interviews and evaluating the empirical findings.

To reach additional level of anonymous security we will not refer to their names or statements that were said during the interviews, i.e. when evaluating the answers from the conducted interviews. Like mentioned earlier, our purpose with this study is to find out the fundamental choice of the bank's online access system, therefore interviews will be most suitable in order to fulfill our purpose.

2.2 Knowledge characteristics

With this report we will deepen our understanding within the area of informatics, in more specific develop knowledge about online banking and how IT-security affects organizational decisions.

Goldkuhl (1998) mentions that identifying knowledge characteristics is necessary during the study, and this done through analyzing and indicating what type of knowledge will be developed. There are wide ranges of different knowledges and for that reason we need to categorize the knowledge. In accordance to Goldkuhl (1998) knowledge can be categorized in the following knowledge forms; *categorical-, classified-, descriptive-, historical-reconstructive, comprehensive- , predictable-, valuable knowledge, normative- and knowledge of characteristics that puts focus on comprehension.*

In general matter, the fundamental form of knowledge is *categorical knowledge* which makes it the dependent variable for the development of the other knowledge forms that exist (Goldkuhl. 1998). In more detail this form of knowledge divides different phenomenons into categories. Nevertheless categorical knowledge may also be seen as an own knowledge form, i.e. independent form of knowledge.

In addition for our report, we will neither find it necessary to describe nor reflect on all the knowledge characteristics that exist, since all the knowledge characteristics are already described in Goldkuhl (1998).

Our goal of the study when developing necessary knowledges will be based on our research questions. From those questions we will find out what kind of knowledge will be essential for our study. Moreover, according to Goldkuhl (1998) by identifying characteristics of different knowledges can create a strategy for the development of the study. When working with this it is fundamental to ask ourselves what kind of knowledge development is essential, and for what purpose?.

To be able to describe certain phenomena, the characteristic of *descriptive* knowledge will be necessary regarding our report. Moreover this knowledge can be both of quality and quantity characteristics, dependent on the characteristics' nature (Goldkuhl. 1998). From our point of view the descriptive knowledge will be created when describing the phenomenon of online banking, through explanations and evaluation of what online banking is and by analyzing different definitions and theories related to the subject.

Concerning our first research questions "What principals are behind the decisions of online banking systems today?" we will need to develop both *comprehensive* and *normative* knowledge, since we want to answer the questions of what and why of the factors behind the decision of online banking system. We want to understand what online access system used today, but also why it is used, what fundamental factors are behind the choice of system, done by the banks.

According to Goldkuhl (1998) *Comprehensive focused* knowledge is of a particular kind of knowledge, where the emphasize is on *what* something is. In more detail, deciding the meaning of a phenomenon and this is done through categorizing the phenomenon into amount of stated characters. Further, the comprehensive knowledge is also essential when explaining *why* a phenomenon is in a specific manner and this is used especially within the area of scientific. The main purpose of the development of the comprehensive knowledge is to study its hypothesis' relations that occur. A common case of developing comprehensive knowledge is examination, where one can evaluate if the hypothesis exists.

With knowledge that will guide one through the study, the *normative* knowledge will be suitable, it consist of rules, guidelines, councils, regulations for acting in different situations, which is also called *method knowledge*. Normative knowledge tells how one should act in a certain circumstances, which leads to a knowledge form with focus on action. Further, normative knowledge is example on models and methods for business- and system development.

Regarding our second research question "What principals will be optional in the future?" about the future aspect of online banking, we find a mixture of *predictable* and *comprehensive* knowledge are suitable, since comprehensive knowledge might be useful for obtaining knowledge about the future and this means that the knowledge turn into a character of *predictability*, through creating presages by applying comprehensive knowledge into a specific situation in order to create some kind of prognosis (presage) for the future events.

2.3 Research approach

In order to fulfil our purpose of this research we choose to investigate the different systems used when customers want to get access to their personal account online.

We have to gain knowledge about IT security and banking by qualitative examination of Swedish banks and reading theories about IT security and also reading about Internet banking security systems. Furthermore we will try to compare different kind of online banking systems outside Sweden.

We are going to conduct our literature study through reading other researches connected with the concept of online banking. Our primary data will consist of collecting information about the subject presented before in the introduction. We will search different databases for articles, more in-depth studies of online banking, read books about different IT-security theories and then connect the theories with studies made of the phenomena of online banking and different online banking cases. We will mainly look at how online banking is done in Sweden.

When searching on the university's own database "JULIA" and using the key words *online banking*, *IT-security* and *internet banking*, both in Swedish and English, we could not find any written work of the subject. Consequently, we needed to expand our research to bigger databases. The first one we used was "Academic Search Elite". Here we could find many articles and more in-depth studies when using the keywords "*online banking*" and" *it-security*". Then we expanded our research to another database called "IEEE Explore". Here we only used the key word "online banking", which also gave us some new articles and in-depth studies. The big difference between these two databases was that "Academic Search Elite" only provide studies made in the US or about the US while "IEEE Explore" gave us studies made outside the US, like Norway and Finland.

The studies we found from both databases all had something to do with different attacks and threats which are a high security issue to online banks, like *phishing* mostly but also different malicious attacks such as *Trojans,* according to the articles or in-depth studies.

More over the two databases gave us results that focus on the importance and benefits of using *biometrics* (using human DNA in order to identify them selves when accessing into a personal account). When relating to our study area we notice that this method could be a possible future security solution for the bank to consider. One established periodical in the university library is the *New Scientist;* hence the information gathered in this periodical is contentiously updated and in addition related to the concept of online banking.

2.4 Quantitative and qualitative research method

Holmes & Solvang (1996) discuss quantitative and qualitative research methods and the differences and the similarities in their research book. Their result shows that there are many similarities with these both research methods, but based on different aspects. The fundamental goal of the two research methods is to give a better understanding of the society we are living in and how individuals, groups and institutions reacting and affecting upon each other. In addition, the fundamental difference is that the quantitative research method transforms the information collected into figures and numbers, while the method of qualitative research is put together up by the researcher's understanding and interpretation of the information gathered.

In more detail, a quantitative research method according to Holmes & Solvang (1996) gives an analytical perspective with formalised and structured data, which is used for statistical analysis. It is objective and the result can be measurable by figures and quantity. An importance notice in this method is that the result is only valid for a short period of time. Moreover, the qualitative research means that the method has a primary purpose to give an un-

derstanding of fundamental information. From this information the researcher is able to perform an analysis with an understanding perspective.

The qualitative research method creates a holistic view with an increased understanding of both the society and the individual situation. The principle of knowledge characteristics, which will be explain further later in this report, is to gain closeness with the respondents and this will be reached through the qualitative research method, because it will give an understanding of the respondents' view of the phenomenon and this through different kind of interviews (Holmes & Solvang. 1996).

The both research methods are tools for creating a better understanding of something, and they can be combined in order to create a foundation of each other or they can also be conducted simultaneously. An immense advantage of the combination of these research methods is that if they give the same result, then they create stronger argumentations, in addition if the results differ then new theories can be developed.

According to Holmes & Solvang (1996) all the units which are related to our study, in our case all the banks offering online banking, will be our population. Furthermore, to be able to conduct a research and to provide reliable and valid information we need to limit the population to a sample. In our study the sample will consist of four established banks in Sweden that offers online banking. These four banks are; Swedbank, Nordea, Handelsbanken, and SE-Banken.

2.5 Choice of methods

In order to fulfill our purpose of this study, we have chosen a qualitative approach of gathering our empirical data, because this approach is most suitable when it comes to fulfill our perspective, gather data related to the managerial point of view.

Firstly, to collect empirical findings we will interview different Swedish banks in order to retrieve a practical perspective of our study. This will hopefully give us information about the principles they have behind their decisions toward their choice of online banking system. This will create our primary data for the study. First we want to find out what type of online banking access system they are using, and why they choose this.

Furthermore, we choose to interview the local banks which constitute of our sample. The reason behind this is to gather information of how they look upon their choice of online access system from lower level of management. Then we will use that information to both help and create a good ground for the interview which we later will conduct on each of the banks' headquarters. At each banks' headquarter we then hope to get in contact with the best suited person to interview regarding the authentication system used by that bank. This will give us reliable information and also valid information; will be explained later in the report.

The qualitative method will consist of conducting telephone interviews with the banks' headquarters and by personal interviews on the local level. We prefer to conduct telephone interviews with the headquarters since they are too far away for us to be able to visit them and also because we want to come in personal contact with the headquarters of each bank from the different banks we have chosen. The process of performing telephone interviews is by contacting relevant people, from the headquarters of each bank, by asking questions which are prepared in advance. The main advantages of choosing telephone interviews are that they can be performed rapid, cheap and gives high answer-frequency among the re-

spondents. Another advantage is that the researcher can follow up the questions raised in the interviews. In addition when conducting telephone interviews the questions can not be of a complex nature, you may neither provide visual pictures, and it can also be difficult to ask sensitive questions.

Additionally, we will make observations of each banks webpage to gather information about the different online banking access system used by each bank.

With the choice of qualitative research method, our study will hopefully give us reliable and valid information about the principles they have behind their decisions toward their choice of online banking system.

2.5.1 Interview

As stated above we will choose a qualitative approach when gather our empirical information, this will be done through interviews, and hence we will conduct qualitative interviews. According to Holme & Solvang (1997) the strength of conducting qualitative interviews is that they are of a more every day conversation and this means a situation where the researcher have the least control to steer the interviewed person. If it, at a later point shows that there are new things we don't feel we have gotten enough information about, then the method is very flexible, meaning it is rather simple for us to go back to the person we interviewed and ask those questions. This means that the analytical part and the empirical gathering often overlap each other in this form of interviews, which is different from a quantitative interview. This is positive for our study since it might be difficult to complete all the interviews as planned. Then this flexibility will give us the possibility to both analyze and interview in parallel, meaning this will help us keep a high validity and reliability even though there might be short on time in the end.

To come up with the interview questions we first brainstormed some questions and then tried to pick out the ones which would help us answer the research questions from the problem discussion. The interview questions for the local banks were going to work as a guide for us to come up with as good as possible interview questions for the headquarters. To see whether or not the interview questions we had come up with was in line with fulfilling our purpose we sent them both to our teacher and our opponent group, in order to get feedback, in order to change them or create new questions.

After the feedback and the research questions was completed then the finale questionnaire was created. This could then be sent to the sample banks in order for them to get an insight of what the thesis is about. This questionnaire served as a guide for us and the bank to be able to set up a meeting to conduct the interview through phones with the headquarters and direct meetings with the local banks in Jönköping.

At the direct meetings with the local banks we used the questionnaire as a guide during the interview and we tried to have one of us asking the question and the other writing the answers down, since we did not use a tape recorder. If the other who was taking notes did not understand an answer they could also ask questions to verify or clarify the answer. During the telephone interview we followed the same procedure only here we only let one person ask the question and the others listen and take notes. We followed this procedure because we did not want any confusion between the respondent and who they were talking to.

Further the subject of online banking access systems is not a subject that we can gather enough information from other written studies and researches to be able to come up with a good quantitative ground to conduct. Furthermore a qualitative interview is more of the characteristic to gather statistical information. Hence that is not the type of information we need. We need a deeper understanding of the subject. According to Holme & Solvang (1997) qualitative interviews will give the researcher a deeper understanding and more complete information regarding the subject if the researcher can manage to come in contact with the right person. This means the choices of respondents is not done by hazard, but are chosen after some certain criteria decided before the interviews are conducted. In our case we have chosen to try and come in contact with the best suited person, meaning a person who knows the most about the online bank and the online banking access system, the specific banks are using today.

According to Holme & Solvang (1997) there are different types of interviews the "respondent interview" and the "informative interview". Where the respondent interview is done with a person who is a part of the phenomenon we are studying and an informant interview is done with a person who is not a part of the phenomenon but knows a lot of the subject at matter. In our case this is a bit hard to know whether the person interviewed is an informant or a respondent, since we don't know whether he or she uses the online bank or only works with it we choose to consider him or her as an informant since this person knows a lot about the subject.

The handling of our empirical material was done through gathering the data received from both headquarters and local banks. After we gathered the empirical material we needed to conclude and compile the information. Since we have promised the banks that the answers they give us will be anonymous we have to present the material in a general way. This means we present the general characteristics the banks have in common and also states differences which exist without connecting any of the information to any specific bank from our sample. To be able to see the common characteristics and also the differences the banks have, we have looked at each question and what each bank have answered. The next step was to presented the similarities and the differences in the empirical findings in order with the pre given questions (see appendix) one to question ten, in a top down approach.

2.5.2 Observation

Observation is data gathered for scientific use, where the researcher with the help of their own senses monitors measuring instruments (Carlsson, 1984).

In our study we will besides gathering empirical finding from interviews, evaluate our sample through an observation of their websites. Moreover we will find out how the different sample banks online banking access system appear online and how the authentication process works. This is because we can not find any literature about this.

2.6 Sample of Swedish banks

According to Holmes & Solvang (1997) all the units which are related to our study, in our case all the banks offering online banking, will be our population. Furthermore, to be able to conduct a research and to provide reliable and valid information we need to limit the population to a sample. In our study the sample will consist of four established banks in Sweden that offers online banking. These four banks are; Swedbank, Nordea, Handelsbanken, and SE-Banken. Moreover the evaluation of these banks will be with emphasizing

on personal authentication process only, which means we will exclude company authentication.

2.7 Reliability and Validity

Reliability and validity are two concepts which help us to develop good research questions by continuously searching for mistakes regarding the development of the research questions and furthermore to look for misinterprets of gathered data (Holmes & Solvang, 1997). This is to gain a higher level of reliability and validity of our work.

The reliability is decided by the accuracy of how our measurements are done and the validity is decided by what we are measuring and furthermore if this is in line with the questions at issue. To be able to keep a high level of reliability and validity we need to continuously check the work we have done with criticism. This means that we can not only see if our work has a high level of reliability and then this will automatically give a high validity. The information can only be reliable if the information measured is valid, meaning that the information can be very reliable if the information or data measured is measuring something else than we want or believe us to be measuring, but it still can not be used to fulfill the researched questions we have. This means that the information or data gathered has to be valid, meaningful for our research questions (Holme & Solvang, 1997).

In order to achieve as high reliability as possible for our report, we will have to carefully conduct relevant questions for our respondents, based on our research questions. It is important that we construct questions that will be relevant for our purpose of our study, and that the questions are made with as little misunderstanding as possible, in order to get answers which our result can be based upon. How we conduct our interview questions can have an affect on our gathering of the primary data.

Additionally, for interviewing the local banks, we will conduct different questions than the questions given to the headquarters from our sample, hence questions that will be more suitable for the local banks.

Reliability can also be measured if the result of our research will be repetitive and this will be done through checking continuously the result critically as mentioned earlier. Furthermore we will also try and talk to the best suitable person in order to get as good answers as possible, which will increase the reliability. High reliable research can also be conducted through comparing other studies, made by other researchers. But since no other similar studies have been done within this research area of online banks, we will not have anything to compare with other researchers.

If we are able to create reliable interview questions, it will lead to valid answers, which in turn will give us a more holistic view behind the principles of online banking access system.

2.8 Actual working Process

From the beginning of this project we decided to conduct interviews with the local banks in Jönköping to gather information about how much they knew about the online banking access systems they use, and to come up with better interview questions for the Headquarters. The interviews with the Headquarters were supposed to be conducted through telephone interviews, which was not achieved in all cases due to that some of the respondents had very less time. Therefore, we solved this by letting them answer through e-mail instead. This was solved by sending them the questions and then letting them answer as soon as

they could, but before a specific date pointed out at the first contact with the respondent. Furthermore this led to that the time frame we came up with from the beginning had to be broken. This resulted in that we had to cut down on the time we had set off to conclude the interviews and also some off the time set off to analyze the theories and empirical findings gathered. Besides this we have been able to stick to the working process presented throughout the method chapter.

3 Theoretical framework

In this chapter we will present theories and other studies made about online banking. First we will present online banking as a subject and move on to how passwords are used and why, but also their weaknesses. Continuing with presenting the authentication process, most secure banks are using today, also new complimenting ways of making the authentication process more secure. Furthermore what new treats are rising and how we can protect ourselves against these new emerging threats.

3.1 Online banking

With the increasing development of technology, and with the benefit of using today's computer technology, online possibilities give the option of saving time and paper work. Both at work and private, one can manage the finances more quickly and efficiently (Bankrate.com 2007). Online banking creates additional opportunities and challenges for the banking industry.

In more detail, online banking is the performance of banking activities via the internet (Answers.com 2007). A good online banking system should not differ much from what a traditional brick and mortar bank offers. The great benefit of online banking is that it is free and the possibilities of accessing your bank whenever it is convenient for the customer, 24 hours per day, seven days a week and requires only a few mouse clicks for any transaction.

Other advantages of online banking (Bankrate.com 2007):

- Ubiquity = even if you are abroad and you want to make any transactions this is possible by just log in to your online bank from any computer.
- Transaction speed = the online bank sites perform and confirm even faster than an ATM processing speed.

There are also disadvantage of online banking that needs to take into consideration:

- The start up process = when starting using the bank's website, it will require identification and to sign a form
- Learning process = some banking websites can be difficult to navigate the first times and need to be explored in order to get familiar with all the functions.
- Trust = one of the biggest obstacle of doing transactions online, doubts occur if the transaction was successful, if the button was pushed once or twice etc.

Furthermore, a good online bank should offer high IT security. The object of having a good IT security is to eliminate or reduce significant threats against its system. The IT security comprise of three basic components; *confidentiality, integrity* and *availability* (Bishop, 2005).

- Confidentiality = the system should be secure by ensured that the system will not be accessed to anyone who do not have the authority, the goal is to keep the information or recourses hidden and this applies especially of the use of computers within government, medicine and law, there are different access control mechanism that support confidentiality (ex: cryptography).
- Integrity = integrity of data is about the level of trustworthiness of data or resources, the goal is to prevent improper or unauthorized change of data, important aspect is to protect a person's integrity, there are two kinds of integrity mechanism;

prevention and detection, the prevention mechanism avoid any unauthorized attempts of changing the data by preserving the data, detection mechanism will discover when the data's integrity is no longer trustworthy through analyzing and reporting the data status.

- Availability = the information or resource should be accessible when desired, a system that is not available considered to be as bad as no system at all, in some aspects the data can also be intentionally arranged to deny accessibility due to security aspects.

3.2 Authentication

According to Bishop (2005) authentication is defined as; the binding of an identity to a subject. The goal of the authentication process is to ensure that the individual are correctly identified by be verified through different security mechanisms. One of the most used mechanisms today is password, which consist of information that the individual must provide to the system, in order to confirm ones identify. Besides the password, information needed to access can consist of the following factors that the system must store, in able to confirm the correct user (Bishop, 2005):

1. what the entity knows (passwords or secret information)
2. what the entity has (a badge or card)
3. what the entity is (fingerprints or retinal characteristics)
4. where the entity is (in front of a particular terminal)

Furthermore, the process of authorize the user continues of obtaining the authentication information from the specific user, analyzing the data, and determining if it is linked with the user.

3.2.1 Security policy and mechanism

According to Bishop (2005) a secure system is a system that begins in an authorized state and can not be entered in an unauthorized state. This will in order require some type of security policy, which can be either formal or informal. A security policy is defined by Bishop (2005) as; "a statement that partition the states of the system into a set of authorized, or secure, states and a set of unauthorized, or nonsecure states". The goal is to restrict what is actually allowed and what is not allowed, e.g. an organization informing its staff of what is permitted to do and not to do in a system.

There are different kind of security policies, but in common they cover all aspects of confidentiality, integrity and availability as described earlier, e.g. different types of security policies are; military security -, commercial security-, confidentiality – and integrity policy (Bishop, 2005).

With different security mechanisms, one is able to implement the security policy into the system, to prevent, detect and recover from the attack. According to Bishop (2005) a security mechanism is an entity or procedure that imposes some part of the security policy. In more detail it endures of a method, tool or procedure to be able to enforce a security policy. How the security mechanism can correctly implement the policy and how the policy itself meet the requirements of the organization, using the system which leads to a question concerning assurance. Assurance is a matter of trust, which can not be quantified precisely,

but it is the system specification, design and implementation that provide a basis for determination "how much" to believe a system, which will be more described in detail below (Bishop, 2005):

- Specification: formal or informal description or statement of how the system should be functioned with "secure" and "non-secure" actions.
- Design: convert the specification into components that will implement them.
- Implementation: With a clear design it is needed to be implemented in order for the system to satisfy its design. If the implementation performs precisely, the program is correct.

3.2.2 Passwords

One of the main authentication mechanism used today is passwords, which consist of information which is linked with an individual and able to confirm the identity of the individual (Bishop, 2005). It is based on what the individual knows, information of what the user supplies as a password and the computer confirms it. The system can only be accessed if the password is correct, then the user's identity is authenticated. The simplest attack against a system providing this kind of security mechanism is to guess the secret code (password). This is called a dictionary attack, guessing the password by repeated trial and error. To be sure that an unauthorized will not access the system, good passwords should be constructed, containing at least one digit, one letter, one punctuation symbol and along with one control character will make it a strong authorization.

There are two kinds of passwords today, reusable – and one-time passwords (Bishop, 2005). Reusable passwords are more susceptible against dictionary attacks. The one time passwords are only valid for exactly one use, by other words it is invalidate as soon as it is used. Two issues occur with one-time passwords, the generation of random passwords and the synchronization of the user and the system.

3.2.3 Passwords in today's society

Using passwords in today's Internet society is not enough at all to be secure, and according to Bill Gates, which said at a computer-security industry conference in February that "password systems simply won't cut it", but we can't switch to more sophisticated methods over a night. Therefore we have to use the world of passwords for a bit longer. The best way for now is to use passwords in a better way. Last year the federal banking regulators approved guidelines for the adoption of other forms authentication regarding online banking access systems, which meant number generators or smart cards (Lemos, 2006).

This is urgent because of the rapid pace at which faster processors and new tools for cracking passwords are improving. As an example of a very popular brute-force password-cracking software is "Jack the Ripper" which now can crunch over a million password possibilities in a second, which only could break a few hundred of the same a decade ago. There is also other technique's, such as the cheap memory, which works as a catalyst for password cracking. There is such a technique known as "rainbow tables". This technique pre-calculates a large percentage of all possible passwords and creates lookup tables consisting of multi-gigabyte which reduce the time needed to find most passwords to seconds (Lemos, 2006).

This rapid paste at which methods are being developed to crack passwords makes up for the importance to use a second method of authentication (Lemos. 2006).

3.2.4 Securing the authentication process

As an increasing number of people using internet to use online banking services as stated before, the level of fraud is increasing. What are the options banks can make and what can be enforced by law (Smart card solutions, 2006)?

3.2.5 Two factor authentication

Banks cannot rely on governments, internet service providers (ISPs) or their own customers to make internet a safer place and thereby make online banking safer. Therefore banking regulators in US, Europe and Middle East was looking in 2005 at the very questionable security with static simple username and password systems. They were then influencing banks that had not started to use the stronger security system, using two factor authentications.

This solution is widely used today by several banks but in different ways, all refers to the two factor authentication (Reavley, 2005).

Two factor authentications are based on the idea of something you have and something you know i.e. your PC or smart card and a pin or password (Smart technology solutions, 2006).

PDAs which generates a one time registration password is an example of a two factor authentication process and is very popular in Sweden. Even though this system has been proven in the field it is a very costly system, due to the fact that the PDAs has to be personalised before they can be given to the customers, and in addition the cost of the PDA itself (Reavley, 2005).

Mobile telephony is proving to be a popular choice as well, especially in Australia, where they uses a text messages based system. When a transaction is initiated the bank sends out a text message with a randomly generated code which then the customer uses to complete that specific transaction. These are only a few examples of two factor authentication processes there exists

Two factor authentication has been enforced by US regulators as the minimum security requirements banks have to use by US banks in the end of last year, 2006. Meanwhile in UK only one bank, Alliance & Leicester, has voluntarily adopted two factor authentication. Hence legislation might be the only way for UK to dramatically change the risk factor. This two factor authentication is becoming an industry standard, but as stated above there are serious weaknesses with password as the common currency in authentication (Smart card solutions, 2006).

Other alternative security measures do exists, such as one time passwords. One time passwords (OTPs) can be generated in two ways. The first uses a mathematical algorithm and making a new password based on the previous one. The second is based on time synchronisation between the client providing the password and the authentication server. These OTPs method makes it harder for outsiders to gain access, and if a fraudster does get access it is only for that single time. This is very costly for banks to implement and this system was also the centre for phishing scams targeting a Swedish bank 2005. What was done

in this scenario was that the customers was sent fake emails with a link to a fake webpage but identical in appearance as the original banks webpage. Here the customers typed in their OPTs and then the phisher could use this to gain a one time access. Another down-side with this system is also that it requires a certain level of customer education (Smart card solutions, 2006).

The last scenario described with the Swedish bank was a so called "man-in-the-middle" attack. All single, two factor authentication and OPTs are open to these type of attacks but also to different Trojan scenarios, which will be described later (Smart card solutions, 2006).

3.3 Emerging bank threats

As it gets harder and harder to crack customer's online banking access passwords, fraud has become an emerging way for thief's to manipulate the customer's transactions. The weapon of choice for a hacker when it comes to fraud is phishing; hence phishing has become a banks biggest threat. As much as two to five percent is drained from banks revenue because of fraud. Phishing is a form of social engineering where the phisher tries to gain the trust of a user and make them believe they are talking with their bank, and then the phisher will try and get the customers personal information and then use that to gain access to the customer's online bank. The methods are getting more and more sophisticated, but on the other hand users are also getting smarter. This is leading to that cyber criminals like phisher are starting to use SSL-evading Trojans; this is Trojans which install themselves on the user's computer which either capture user log in credentials or manipulate transactions after a successful log in. In both these scenarios the SSL connection remains intact; these attacks can also be called "man-in-the-end-point" attacks. The problem here is that ever since Netscape developed SSL in 1996 consumers have been told that a SSL-connection is safe, which is indicated by an icon in the web browser. What the SSL states is that the connection between the network card in your PC and the network card in the bank is not compromised (Grimes, 2006).

This new tool, SSL-evading Trojans, is as it seems, becoming the hacker's favourite weapon. Hence it can bypass any authentication scheme. The latest way for banks to prevent hackers to gain access by creating more complex authentication schemes, two-factor authentication solutions, which is used in different ways today by banks, i.e., smart cards or number generators do not help when it comes to the new breed of SSL-evading Trojans. According to Bruce Schneier, "It is not a problem of authentication but one of transactional authorization". Because it does not matter how hard one makes the authentication, since this new malware simply waits until the authentication is done and then manipulates the transaction. Hence ones your computer is infected you can not stop it (Grimes, 2006).

3.3.1 SSL-evading Trojans

As stated before this maleware can bypass the secure and authenticated tunnel between the bank and the customer, which is the backbone of today's online banking, and also other institutions. There are three different types of SSL-evading Trojans (1) is the credential-stealing which is very similar to the more usual password stealing Trojan but the credential one has a twist to it. Instead of just recording keystrokes and send them to the attacker like the usual, these Trojans also subverts authentication methods as on-screen keyboards, in a short way of explaining this, the software takes snapshots of the users screen when a user clicks in previously authenticated areas, these pictures are then collected, zipped, and sent

back to the attacker. (2) Is the bogus SSL Trojan which is easier to understand. These Trojans installs themselves and then searches the users' browser cash memory to find financial and bank web sites (Grimes, 2006).

Then when the user is to log in to there online bank the Trojan intercepts and redirect the user to the bogus or fake web page. Then the Trojan simply sends the information typed in by the user both to the attacker and the real bank. (3) Which is the most dangerous are the transaction based SSL-evading Trojan and also the most sophisticated ones. These Trojans wait until the user has successfully been authenticated by the bank which entirely eliminates the need to bypass or capture a user's authentication information. What the Trojan then does is that it manipulate the transactions made by the user, which means what the user believes is happening is actually not happening (Grimes, 2006).

These are very hard Trojans for antivirus programs to detect as well because they are so called "one-offs", meaning each such Trojan is encrypted or packaged so that each Trojan becomes unique. The only way for users to really be sure of not get infected is when they stop running un-trusted code or when, which might even be a better solution, banks adopt back-end defensive mechanisms which moves beyond the normal authentication process used today (Grimes, 2006).

3.4 Biometrics

When identification by physical characteristics is not secure enough when accessing into a system, other secure measures will be required, such as recognizing people by their voices or appearances. This method is called biometrics and it is more precisely automated measurement of biological or behavioural features with the goal of identify a person and eliminate errors in authentication. The process consist of the user which given an account, log in to the system and the system administration capture a set of measurements that will identify the user through biometric authentication mechanism. Common characteristics of biometrics identifying are fingerprints, voice, eyes, facial features, and keystroke dynamics (Bishop, 2005).

When authorizing through fingerprints, a scanner is identifying the friction ridge structure of the tip of the finger and detects the part of the finger that touch the chip raise. The data will be converted into graphs, where the ridges can be represented by vertices and vertices corresponding to the closest ridges.

Another word of authentication by voice is speaker verification or speaker recognition, and this means verification of a speaker's voice characteristics or verbal information verification. In order to identify the speaker, statistical techniques will be used to test the hypothesis which is claimed. The verbal information verification is identifying the content of sound, where the system ask the user a set of questions such as "What is your father's name?", "When were you born?" etc.

Additionally, another biometrics mechanism is identifying eye characteristics, which in more detail identifying the iris and the retina. Due to the pattern of the iris, this makes every human unique. Using retinal scans, it can identify the uniqueness of the patterns which is made by blood vessels at the back of the eye. This can be highly intrusive, since it will require a laser beaming onto the user's retina. Authentication by eye is typically used in the most of secure amenities (Bishop, 2005).

Authentication through face recognition consists of several steps. It starts by locating the face, where the result image is compared with the relevant image in a database. However, facial features such as hair and glasses can make the recognition harder for identification.

The last mechanism for biometrics identification requires signature based on keystroke intervals, keystroke pressure, keystroke duration, and where the key is stroke. Moreover, the keystroke mechanism can be both static and dynamic, which consist of a process of first static recognition through typing of a fixed or known string during the authentication time. When the authentication is done, an attacker will be able to capture the connection without any detection. Secondly, the dynamic recognition is executed throughout the session, in order for the attacks to not be possible.

In addition, the authentication using biometrics uses the technology to measure and analyze human physical and behavioural characteristics for confirming the right user to the system. Unfortunately, two assumptions has been identified which underlie this belief that attackers can not authorize into the system that uses biometrics as identification. Firstly, it is essential to check if the biometric device is accurate in the environment in which it is used, in order to prevent the unauthorized to gain access by accessing through a mask of another person's finger. By observation, this trick can be detected. The second assumption is the challenge of constructing the system tamperproof, which means to secure the transmission from the biometric device to the computer's analysis process. The risk is that the unauthorized can legimitate a suitable authentication and repeats it later to gain access (Bishop, 2005).

In order to improve the accuracy of biometric authentication, several researchers combine the different techniques, i.e. combined voice sounds and lip motion with facial image. The results from the research point to that in order to achieve higher degree of accuracy, it is essential of using more than one single characteristic of biometrics can be attained (Bishop, 2005).

3.4.1 Biometrics today

For improving the security within different business, using measurements of biometrics has become a great benefit. One of the techniques used today is using fingerprints to confirm the user when accessing a personal account. But as improving the security, the threats of the system rises as well. Fingerprint scanners are increasingly used, but fake fingers made of silicone, that biometrics experts today are trying to beat (NewScientist, 2006).

In addition, digital security has changed the security within many different businesses, where fingerprint scanners are increasingly used to control access to buildings, devices and services. The threat is that fingerprints can be stolen for example by physically "lifting" them or by hacking into the biometric code stored on a device such as a laptop. Fingerprints can be prevented from be stolen by accessing bank accounts or computer files, with a security system that has been developed by a London-based company. The system combines the fingerprints recognition with a version of traditional PIN code, in order for the thief to not be able to know the correct sequence (NewScientist, 2006).

Lately biometric experts have introduced the approach of using *electronic nose,* which has been later discovered within security. This security tool will be able to distinguish the unique aroma of a human skin. Electronic noses have already been used when monitoring pollution and determining if food is spoilt. David Maltoni at the University of Bologna tried the electronic nose, placing it inside a fingerprint scanner and his study showed that

the electronic nose could accurately sense the difference between real and fake fingers (Biever, 2006).

More and more studies have occurred, since the need of biological detection has grown for improving the security. According to NewScientist (2006), a biometric expert at the University of Kent at United Kingdom states that more biological detection tools are needed in the future (Bishop, 2005).

3.5 Strategies and management challenges faced by banks

A study made in UK for about ten years ago, tried identifying the different approaches UK banks were taking towards implementing electronic banking, and the strategies behind those approaches. Moreover the study identified the problems and concerns managers would experience in that area. We say electronic banking here because this refers to other alternatives then only banking over internet, hence online banking. Four different types of electronic banking were defined. (1) PC private dial-up services, where the bank offers property software to the customer who installs this software on the computer which then provides an access to the bank through a directly linked modem. This was the approach the majority of banks choose in UK in 1997. (2) Managed Networks, this is when the bank makes use of a network operated by another party. (3) Internet, which is the same as the major banks in Sweden are using today and which we refer to as online banking in our study. (4) TV-based services which are when the customer can get account information through their satellite TV.

The interesting findings from this research is the factors behind the decisions banks made to why implementing electronic banking then and what they thought the future for online banking would look like. According to the study which was made through ten personal interviews, semi structured, from seven of the major banks in UK. They believed that the future would go towards using internet based services; hence online banking and that the use of smart cards would be the most popular choice. They don't mention any thoughts about the PDA system (Daniel & Storey, 1997).

The biggest reason for why internet services would be more popular in the future back then was because the existence of additional services and because customers would not need direct personal contact to do transactions which we can refer to as standardized and low level complexity and where a low level of advice is recognized (Daniel & Storey, 1997).

There are seven major strategies found towards implanting electronic banking;

1. To protect or enhance reputation
2. Added Value for customers
3. Means of attracting new customers
4. Demand from current customers
5. Competitors are launching the services
6. Cost savings
7. Enable mass customization

There are six management challenges recognized;

1. Customer acceptance
2. Integration with other channels
3. cost savings

4. Pricing strategies
5. The impact of intermediaries
6. Top management support

The reason behind why the banks wanted to implement the electronic banking was to be able to attract new customers and moreover to be able to compete with the other banks that were doing it. Meaning, if one bank implements a new online access system, the others have to, in most cases, follow. Otherwise they will most likely loose customers due to lacking competitive advantages. The major concern was how well the public would accept and trust it and when and at what rate online banking would grow from a service utilised only by a minority of customers to become a major distribution channel. Today it is a fact that it is a major distribution channel and that was what the banks predicted then, hence our question what are the banks predicting today, which are to be investigated by this study (Daniel & Storey, 1997).

3.6 Different security guidelines offered to users in future application

There have been several security guidelines offers for users and especially for bank management to take into consideration, a future application that would be a potential interest, and something to take into consideration for all parties involved in online banking, (both bank users as well as the internal bank security management) is biometrics (Hines, 2006). According to the article "Bank to serve as virus firewalls", there are numerous antivirus application offered for online users directly via their websites, this in turn is a perspective that bank considers will increase more peoples interests in doing business online.

Furthermore in the future there are many possible ways for banks to reach other possible solutions for security that also could be applied by the customer themselves. By for example encouraging users to update their security software more frequently could be a way to create benefits for user's security when doing business (Hines, 2006).

In addition these security tools or guidelines that could be taken into consideration by banks for their users are (Hines, 2006);

- By offering free online security tools
- By supporting third-party applications
- Reselling shrink-wrapped software
- By collaborating with ISPs to create secure links
- By adopting two-factor authentication

Furthermore a primary driver for banks is to attract those people that have internet access, but do not use online banking services; studies have showed that the biggest reason for this is that they do not do this because of security worries (Hines, 2006).

In the article "Cost of securing people's privacy" a discussion made by analysis Kelly (2005) about the different agencies and the need to take additional security measures, and more importantly how much this measures will cost to implement enable to protect people's privacy account when using online banking (Kelly, 2005). The aim of this discussion is that these agencies need to concentrate on the so called legislative bill, meaning additional security.

Moreover, it is important to know that the aim of this legislative bill is that it needs to function like additional security protection for consumer privacy. This subject is a constant challenge for online banking to handle (Kelly, 2005).

To be more specific according to Kelly (2005) there are four layers; at layer one he mentions the ability to interact with network access, this includes physical access. Furthermore at layer two discussions is made about the traffic that passes through the whole statewide network because of the fact that the statewide network is not to be trusted according to Kelly (2005), the third layer consist of host to host connectivity via TCP/IP Kelly (2005) believes that legislators would not understand this level of discussion. The level four is the biggest concern for the agencies of all the layers. To reach additional security the need for encrypted internal e-mails is necessary; moreover every database that contains personal information needs to be encrypted as well.

3.7 Relevant theories

After gathering the data for our study we find that areas such as online banking, emerging bank threats, authentication, and future solutions are theories from our theoretical framework which are relevant to help us analyze, and answer our research questions.

Online banking concerns of IT-security, in more detail the three basic components of IT-security as explained by Bishop (2005). When searching about IT-security we find that banks are exposed to emerging threats. We identified a new kind of Trojan threat, the SSL-evading Trojan described by Grimes (2006). Because of the fact that when gathering information about threats these threat were the most interesting in our study area and therefore SSL-evading Trojans became of interest for us. Furthermore this theory will most likely also be of great interest when analyzing the answers from the empirical findings.

Another significant area that we find appealing concerning online banking access systems was authentication, in more detail the theories found about two factor authentication in an article written by Smart card solutions (2006) will be of relevance for our study, since this two factor authentication explains the online banking access system used today. Furthermore this source has not been one of the most relevant theories regarding our analysis but of great importance to be able to present the different authentication processes in use.

When concerning the future solutions and what principles will be dominating in the near future, we found both literature and articles about the use of biometrics and the advantage using it within online banking. The theories found about biometrics authentication was from Bishop (2005) and articles from New Scientist. This will help us answer our wonder about how the future may look like for online banking.

4 Empirical findings

In this chapter we will first present how this report has actual gone through, compared to our planned method, from earlier chapter two. Later we will present the data we have gathered during our research of the four banks. First we will present the different authentication processes in use and continue with findings, regarding the principals behind the decisions, made from interviewing local banks. The most interesting findings are presented last, the findings made by interviewing each banks headquarters responsible for online banking.

4.1 Observations of the banks websites

Information regarding what type of online access systems in use by the different banks from our sample is information they don't write about for the public, as far as we have concluded. Therefore we had to make observations of each banks website to be able to gather information about how the authentication processes for private users are done. The findings are presented below and furthermore copies of the web pages can be found in appendences 1 to 5.

4.1.1 SE-Banken

According to observations of SE-Bankens (Skandinaviska Enskilda Banken) webpage we can conclude that the bank uses a PDA which they refer to as a "digipass". They also provide a guide how to log in (see appendix 1). This PDA is used by the customer to generate a password by entering two different hazardous numbers each time the page is updated. This password then is entered together with the customer's personal number in order to be authenticated by the online access system.

www.seb.se

4.1.2 Swedbank

When observing Swedbanks webpage we find that the bank also provide a guide for log on (see appendix 2), to get access. The customer has to type in their personal number and then choose PDA as authentication; this is called "step 1". Then the user continues by clicking continue, the next step is called "Step 2" and here is a hazardous control number generated which the user is suppose to enter in the PDA which then generate a new number which is the final number and is typed in on the webpage. This number together with the personal number and the hazardous number gives the user authentication.

www.swedbank.se

4.1.3 Nordea

By observing Nordea's webpage we can see that bank are using what we refer to as smart cards. First you choose to log on private and then a page with three different types of authentication process appears. The first one is the main one and the one we will refer to, the other is just compliment when smaller transactions is to be made. First the customer need to type in a personal number and then a personal code, and in accordance to this the code generated by the smart card (see appendences 3 & 4).

www.nordea.se

4.1.4 Handelsbanken

By observing Handelsbanken's webpage we see that the customer needs a username and a personal code. This is all we can see when looking at the authentication process on Handelsbanken, however by reading about their security information we can conclude that they are using what we refer to as smart cards (see appendix 5).

www.handelsbanken.se

4.2 Interview with local banks

The purpose with interviewing the local banks was to receive a perspective of how much these local banks actually knows about the authentication process that is in use today. Moreover, finding out the decision made about the online access system and on which level these decisions are made. Furthermore, how these decisions influence the choice of online access system. We also want to know if they know how to handle different incidents that may occur. To see details of the questions asked (see appendix 7) from the interviews made at the local banks, Nordea, Handelsbanken, Swedbank, and SEB, in Jönköping. The interviews were conducted with the local office manager or head of the private market for the local bank.

We have found that there is no single person with a superior responsibility for the service on the local level. They all refer to their headquarters and in most cases a specific central department. From a local level the banks does not have any influence on what system the top management choose or how to change it in a near future, hence suggestions are not pushed from lower parts of the organizations to influence the upper management, but they support the upper management in their decisions and have trust in them when decisions are made. The responsibility is distributed in a decentralized level, i.e. local bank offices are responsible for the updated information on the website concerning their customers. This makes the bank have a close relationship to their customers.

When asking if they know how many that is working with the online banking service, meaning persons managing the service, the answers differed in two ways between the banks. Some banks made suggestions on how many was working with it, while others answered that they did not have a clue.

Furthermore what was very interesting when we asked the question of how much they know about the authentication system in use, all banks answered very differently. As a conclusion all answers could be referred to the same belief, that they had a very safe system, maybe the safest today. Moreover the answers could differ somewhat, some banks suggested that they had a really practical system while others pointed out the availability, hence it could be used anywhere in the world from any computer. Furthermore why the authentication in use had been selected by the banks headquarter and the ones responsible for that decision, none of the local respondents could answer on. They all believed the reason for this was because it was the safest and best solution for them.

How the local banks believed that their online banking should be viewed by their customers was very different from bank to bank. But in general they all referred to some level of service; i.e. best online bank available, or the most flexible, safe, and available, or working for the customer by providing complements to different type of channels to conduct transactions.

When managing the incidents the different bank organizations handles these in a different way; i.e. an investigation group or special departments were these issues are handled. In general for all banks they need evidence on the incident and furthermore the customers get the money back in almost all cases. As some banks have said, rather give somebody the benefit of the doubt, in order to create a trustworthy relationship with the customer.

When asking about the possible changes for a future authentication system, the answers differed. Furthermore, no general conclusion can be drawn in this specific question. While we know that this might be because the local banks do not have any influence on the system in use today, therefore they wont know much about future strategic directions, hence the answers is built upon the interviewed persons believes.

Some banks stated that their online banking service is continuously changing due to meet new demands and safety recommendations, but no immense changes will occur in a near future. While others said that they are pleased with the system in use as it is today, and to change that system would not be a possibility this early due to the costs of implementing a new system or even compliment the online service in use today.

After conducting the interviews with each bank's headquarter, we found that there are approximately 30-50 persons working with the service of online banking. Of this amount of staff they are supplementary divided up by different functions just to mention some; system developer and technical customer support.

4.3 Interview with headquarters

In general all the banks believe and strive for that the online banking service will in a near future become the most important channel for them to distribute banking services to their customers. To achieve this they all also believe they need to have an on-going development process of the online banking service. Since customer demand is continuously changing and also the security needs to meet new higher demands all the time due to new emerging threats. Some banks even states that the security is moving towards becoming almost 100% secure.

On the question of how their current online banking access system works we can make the general assumptions that the observations made are in line with the answers from the interviews with the headquarters, but one of the banks had an alternative solution to the authentication process described in the observations. This was a client based authentication process, meaning the customer needs to use the same computer with specific software to be able to log in. Furthermore, the answers were of a more technical character. This confirms that the person interviewed knows a lot about the online bank and the access system.

All banks answered almost the same on the question whether or not they have developed the online access system by themselves. All banks have more or less developed them by themselves. Some banks had used consultants and one had further developed an international standard to meet their needs.

On the question of what type of factors and fundamental decisions based choices, which their choice of online banking access system to use, they were all talking about the trade off between security and availability. Some banks said the availability was very important in line with an "enough" secure service. Other banks said that the security was their number one factor, but still keep a high degree of availability, such as mobility and flexibility. Except these factors the banks need to take into consideration the continuously changing market

i.e. the fact that if one bank implements a new and improved system the others have to follow due to sustain their competitiveness and keep their customers.

All banks have a specific department which handles all incidents that the customer might be exploited too. Furthermore if incidents occur the customer will in all cases be compensated which can be seen as a safety net for the customers. Furthermore all banks are continuously working with informing their customers about how they can protect themselves against different kind of threats, such as Phishing and Trojans.

On the questions of whether or not the banks will further develop their security measures they all stated that it is an on-going process, the current situation is based on increasing the customers security.

In future authentication the banks stated that they believe they have a strong enough trustworthiness to meet the demands from the market today. But they are considering new ways to reach a higher trustworthiness on the authentication process but to do that they need to know what type of threats are emerging. Biometrics is nothing which the banks have taken into consideration in a near future development, but the banks have an awareness of this type of technology, and have in some cases even been offered to implement this as a newer solution.

4.4 Critics of empirical findings

We are aware of the fact that the empirical findings we collected are not objective in the sense that the respondents answered subjectively. This effect is due to that they do not want to talk negatively about their own system. Meaning they want to bring out the positive sides of the online banking access system they have in use. Therefore we tried to be clear on that the answers would be anonymously, which would make the respondents feel less reluctant to talk about some negative aspects and be more objective in their answers.

5 Analysis

In this chapter we will connect the empirical findings with the theoretical framework to be able to come up with interesting facts regarding our problem statement and purpose. First by discussion the online banking as an introduction and then continue with try and discuss the factors behind the decisions and then future solutions.

5.1 Online Banking

Online banking is the service that banks offers to their customers, it is a complimenting channel to the traditional way of managing finance matters. Since today's society is changing in line with the rapid changing technology makes it an immense service for the banks to maintain and further develop in order to keep up with the different possibilities and threats that the banks may face.

Our sampled banks experience this rapidly changing technological environment, some had also been faced with the different threats, such as Phishing, and Trojans, but they also believe that they covered this threats in a highly secure way, it is not possible for the banks to avoid the risks of facing different and emerging threats. The banks claimed that it is more of a social issue than a technological matter; with this they meant that it is hard to verify and confirm the correct user.

5.2 Factors behind principles

When going to the local banks and conducting interviews we wanted to find out how much they know about their online banking access system and how much they can influence the decisions made by the headquarters. The interviewed confirmed our believes, hence that they did not have anything to do with the decisions made by the headquarters. But what is interesting is the fact that they do not even give suggestions to the headquarters since the local banks have the most contact with the customers, meaning they should best know what the customers want from an online banking system.

From what we have found out the customers have less to do with the decisions made by the headquarters. This is probably because they know very little about such systems, but on the other hand a customer want an online banking access system which is easy to use and to understand. Therefore when the banks decide on what type of online banking access system to use they need to have the customers in mind. Meaning even though the customer do not directly influence the banks in their decisions, the banks need to meet certain criteria to both keep and receive new customers, in order to reach competitiveness towards the other banks. Hence they need a customer friendly and safe system.

Whether or not they want an available system or a usable system, of course safety is a factor which needs to be addressed in every system. Furthermore, the banks can make systems safer by different authentication processes i.e. use client based applications, but this will strongly affect the availability of the system. The customer will be bound to a specific computer with specific software; this means that the customer must carry that computer with them everywhere where they want or need to use the online bank. After our interviews with the headquarters we found out that one of the banks actually used such a system, but had a two factor authentication system in use as well due to the flexibility and availability. The reason behind this was that they believed that when their customers do

their banking transactions over the internet they do them from the same computer in most cases, which according to them is from the home computer.

5.2.1 Confidentiality

The trade-off between confidentiality, integrity and availability as discussed by Bishop (2005) in the theoretical framework can strongly be connected to what principles the banks base their decisions on when implementing an online banking access system. What seems to be the most interesting principle for banks to consider when deciding of what type of online banking access system to use is the availability and also the usability, hence the integrity and availability presented by Bishop (2005). This is interesting because the safety, hence the confidentiality, is also very important but seems to come in second when deciding of implementing an online banking access system. This might be due to the fact that most banks today are satisfied with the security they have. To illustrate some reasons why banks feel this satisfaction, we will continue with a discussion about this under "securing the authentication".

5.2.2 Differences between facts and empirical findings

Furthermore what is interesting is the fact that they all stated that they are satisfied with their online banking access system and states that they have good protection against all possible threats. This is interesting because of the findings which Grimes (2006) talks about, hence the new emerging threat of SSL-evading Trojans. This new threat is very tricky for banks to protect themselves from since this kind of threat can not be deflected by password authentication, not even the two factor authentication (Reavly. 2005). When talking about possible threats with the banks the awareness of this new type of threat was lacking. This new threat does not affect the SSL security which the banks webpage offers due to that the Trojan only compromises the transaction when it is between the customers and the banks network cards. Therefore it becomes a matter of transactional security and not one of an authentication problem. This might depend on that most banks both believe there online banking access system are safe and also why they don't have an awareness of this type of attacks. To be able to protect the customers from these new threat the only way that exists today that we are aware of are to have an antivirus programs which stop these types of Trojan from entering the computers, mainly the customers computers. But the Trojan is hard to be stopped even by modern antivirus programs because of the fact that they are, according to Grimes (2006), so called "one-offs". Therefore this might call for a new technological security development to be able to guarantee the transactions as well as the authentication in a near future which the banks as it is today do not believe is needed.

5.2.3 Securing the Authentication

Accoridng to Lemos (2006), passwords is not enough to make an authentication system 100% secure, this is also recognized by the banks. But they all agree on that the online banking access system they use today are "enough" secure to be able to meet today's requirements. This is probably because all the banks in our sample are using the two factor authenticating process presented by Reavly (2005) in the theoretical framework, which can increase the confidentiality. By using this they can eliminate the easiest code cracking attempts by hackers, and most other more sophisticated code cracking attempts. This has led to the emerge of phishing attacks, but according to the banks we interviewed, it is very un-

common that these type of attacks ever succeed. We believe this might be due to the fact that the banks are very aware of these type of attacks and therefore they work with informing there customers of how they can protect themselves, e.g. they tell their customers to never give out authentication information in a e-mail or answer to such question when someone calls and asks for their personal access information and pretend to be from the bank. If such an attack should be a success the banks will in most cases compensate the customer by giving back what was lost. This can be seen as a safety net for the customer, hence they know the system is safe, not 100%, but they know that if something does happen they will probably not suffer from such a loss. According to the banks this has to be done because online banking is a service and if they would not compliment the customers they would loose them. By knowing this as a customer this leads us to believe they are more interested in a very flexible and user friendly, hence available and usable system instead of having more security and harder to access and use. This is some of the factors mentioned by the banks when arguing for why they chose the type of access system they have. The trade off between availability and security, hence confidentiality and availability presented by Bishop (2005), is an on-going process but we can see that the most important factors might be the availability and usability when offer such a service.

Furthermore the banks stated that they are dependent on distribution channels such as the post office when new smart cards are needed by the customers, hence the smart card can be picked up at the bank or the post office. This is something that we find rather annoying for customers since they need to plan ahead when using the smart card. This is a problem all customers with a PDA will not have, since this is working all the time when there are batteries, but they will last longer then smart card will before it needs to be switched. On the other hand there is more work if one customer should drop the PDA since those are specifically connected to the user.

According to most of the banks they stated that they are pleased with their system they have in use today. But if one of the banks should change their online banking access system in a near future, according to Daniel & Storey (1997) would most likely the other banks have to follow and also change their systems to be able to continue and stay as competitive as possible in the market. This has also been confirmed during the interviews with the banks headquarters, which stated the same thing as the authors.

5.3 Future solutions

In a perspective of how the future will look like concerning the online banking access system the banks believe that the used online banking access system is already according to them almost 100% secure, and most of their customers are satisfied as mentioned earlier. Moreover, the results from the interviews from the headquarters illustrated that our sample banks are satisfied with their online banking service. They believe that no drastic changes will be necessary in the near future. In almost all of the incidents the result has shown that the main reason why incidents occur is a matter of a human perspective. Hence it is not a matter of seeing the online banking access system from a technological safety concern even though the safety perspective is a high priority from the banks point of view. In addition, the banks argue that it is a concern of customer awareness, meaning that the customers have to be more alert of the fact that they are responsible for their authentication in the sense that they have total responsibility for personal authentication information. It is therefore necessary for the customer to be aware of the security policy, as Bishop (2005) states what is actually allowed or not allowed to do in order to additionally secure the customer's authentication.

We have found that the main diffrences between what both Grimes (2006) and Hines (2005) states about only using passwords as security mechanism for authentication is not "enough", they suggest several guidelines towards different compliments. In comparison, between the empirical findings and theoretical framework the banks states that their online banking access system today is almost 100% secure, and that the security mechanisms they are using today is "enough" for the authentication process.

5.3.1 The new emerging threat

Because of the fact that the banks have little awareness of the new emerging threat SSL-evading Trojans, they are living in a state where they do not feel the need for dramatically changes of the authentication system they have in use today. By increasing the banks' awareness of the emerging threat this will lead to the need for developing new security measuments in order to meet this new transactional threat, the so called "man-in-the-end-point" attack. One problem of why the banks lack awareness of this kind of threat might be due to that all the awareness is towards the biggest threat today, namely phishing which is, discussed by Smart card solutions (2006) a "man-in-the-middle" attack.

As stated by the banks themselves in order to know what kind of threat to protect ourselves from in the future, we have to know what kind of new threats we will bo exposed to. We believe that the "man-in-the-end-point" attack, as discussed by Grimes (2006), is the most important threat to take into consideration in the near future or even today. Therefore we believe this calls for a new focus in security issues and this might hopefully increase the awareness for the banks' IT managers of what new kind of threat that is emerging.

5.3.2 Biometrics as a future solution

The new technology within the banking industry provides new ways of authentication; one is the use of biometrics. This is an additional way to secure the identifying of the individual when authentication is done through biological characteristics, such as fingerprints, eye, voice, facial features etc. Instead of only using two factor authentication, it will increase the security of identifying who the individual is by verifying their fingerprints or the eye retinal for example.

From our empirical findings, we find that the banks are aware of this new technological solution based on biology. In some cases some banks have also been offered to implement this new authentication solution, but they stated that this is not something to take into consideration in the near future, due to the reason that this would be a to big project for the banks to implement in a near future. Another reason can be that this is of a high economical concern for the banks to provide this kind of solution for their customers. Also due to the fact that it would be of a great impact for the customers, regarding needs e.g. safety; they need to feel safe with the system and knowledge about the biological authentication. This might become a compliment as an authentication process in a period of ten years maybe.

6 Conlusion

Below we will present the findings we have discussed throughout the analysis and we will present them in a chronological scheme with what we believe is the most important finding at the top and the least important finding at the bottom for our study.

- Lack of awareness concerning the new emerging threat of SSL-evading Trojans, which is a matter of a transactional challenge and not one of an authentication challenge.

- Trade off between confidentiality, availability and security in all decisions regarding the online banking access system. The factors of what all the banks take into consideration when implemented the systems are security and availability, but the availability seems to be of a slightly higher importance. All this is based upon customer satisfaction.

- Passwords are not enough, but most banks are pleased with the two factor authentication process used today.

- The banks believe they need to have an on-going process of developing the systems in use to be able to meet new threats.

- Can't come up with new solutions before threats emerge since then they won't know what to protect themselves against.

- The solution of using biometrics authentication is nothing that will be implemented in the near future, but something that the banks take into consideration as a possibility in the future of five to ten years.

- PDA – more availability for the customers due to that it last longer than a smart car and you can bring it everywhere.

- smart Card - cheaper for the bank, less availability for customers, especially when traveling for example. Dependent on other distribution channels e.g. the post office.

7 Reflections and further discussion of future topics

The purpose with this report has been to try and identify the principles behind the decisions of what online access system to use and furthermore to try and identify the future principle or principles that might become dominating in the future. We have not succeeded in a perfect way of finding these information but have been able to present a study which brings up some new and interesting findings regarding how banks make their decisions regarding an online banking access system, furthermore also what they are aware of when it comes to different existing and emerging threats and what the future seems to be striving towards.

As mentioned in our method, we will have to consider throughout the study the reliability and validity of both the gathering of our theoretical framework and empirical findings by continuously checking with criticism.

In order to reach as high reliability for our theoretical framework we gathered trustworthy sources within the subject of IT security and online banking. Regarding the empirical findings we believe we attained reliability through accuracy, analyzing and compiling the answers from our interviews. This has been done by the whole group attending the interview occasion where at least two of the group member was taking notes and the third one hold the speech with the respondent. The answers could be interpreted afterwards by comparing the notes, in order to create as reliable conclusions as possible.

We believe we have achieved the goal of a valid study, through using the chosen method by interviewing respondents from the four banks. We came up with a good result through compiling what principles the banks rely on in their choices, and suggestions on further development of today's online banking access systems. The questions made were created in a good way and in line with our research questions. For that reason we believe we succeeded answering our research questions in a pretty good way.

What could have helped us to present more accurate information regarding the principles could have been to come up with more precise interview questions regarding the principles behind the decisions, e.g. why do you believe that your system is better than i.e. a smart card system, if they are using a PDA system. In this research we have only identified the general principles behind the decisions and not the specific factors connected to a specific access system such as the PDA system or the smart card system. But as we have understood both these systems provide very similar security solutions, hence a two factor authentication solution, therefore we do not believe that the security is a reason behind whether or not the banks choose one before the other, it is probably more of a strategic or economical matter and of course to some extent a matter of availability and flexibility.

When concerning the economic point of view, we have decided to exclude this from our study since we believe that this would be out of our field of study.

What can be further investigated about this field of studies might be to find out more specific differences between these types online banking access systems in use today, and also the pros and cons with these systems. This can furthermore be seen from either a customer perspective or a banks perspective, and also continue and follow up on the biometrics as a new authentication tool. Another very interesting subject to investigate is the matter of transactional threats described by Grimes (2006) that banks are facing today. What is the banks awareness of these new threats and how will banks solve this type of challenge.

Suggestions on research question can be:

- What are the major differences between the most used Swedish online banking access systems?
- Will biometrics become a complementing technology in the future, to be able to secure that the right person is being authenticated?
- How can banks solve the challenge of transactional threats?

Referenslista

Andersen. E.S, (1994) *Systemutveckling – Principer, metoder och tekniker* . Lund.studentlitteratur

Answers.com (2007) *Online Banking.* Retrieved March, 12 2007, from *http://www.answers.com/Online%20Banking*

Bankrate.com (2007), *what is online banking?*. Retrieved March, 12 2007, from *http://www.bankrate.com/brm/olbstep2.asp*

Bell, J. & Opie, C. (2002). *learning from research getting more from your data.* Printed in Great Britain by St Edmundsbury Press Limited. Bury St Edmunds, Suffolk.

Biever, C. (2006) Fake fingers no match for scanner's electronic nose. *Technology.* (p. 22) www.newscientist.com

Bishop, M. (2005). *Introduction to computer security,* Pearson Education, Inc US.

Carlsson, B. (1984). *Grundläggande forskningsmetodik för medicin och beteendevetenskap.* Norstedtsförlag AB, Stockholm.

Daniel, E. & Storey, C. (1997). *On-line Banking: Strategic and Management challenges.* (p. 890 – 892) Elsevier Science. Ltd. Great Britain.

Ejvegård. R. (1996). *Vetenskaplig metod.* Printed in Sweden. Studentlitteratur, Lund

Goldkuhl. G. (1998). *Kunskapande.* Internationella Handelshögskolan i Jönköping. Centrum för studier av Människa, Teknik och Organisation (CMTO). Linköpings universitet

Grimes. R. (2006). E-commerce in crisis: When SSL isn't safe. *Infoworld.* (p. 27-31)

Hines. M (2006). Banks to serve as virus fiewalls. *News&Analysis.* Eweek.com (p. 26)

Holmes, I.M. & Solvang, B.K, (1996). *Forksningsmetodik- om kvalitativ och kvantitativa metoder.* Lund.studentlitteratur

Internet.com (2007). *Phishing* Retrieved February, 22, 2007, from *http://www.webopedia.com/TERM/p/phishing.html*

Kelly. C.J (2005). the cost of securing people's privacy. *Computerworld.* Computerworld.com. (p. 31)

Lemos, R. (2006). Password Policies, *PC Magazine*: *Security Watch.* (p. 116)

New Scientist. (2006). Keep your fingers out of my account, *Technology.* (p. 29) www.newscientist.com

Nigel, R. (2005). Secure online banking, *Card technology today.* (p. 12-13).

Pcmag.com. The independent guide to technology (2006). *Trojans* retrieved February 21, 2007, from *http://www.pcmag.com/encyclopedia_term/0,2542,t=Trojan&i=53178,00.asp*

SFS (1998). p. 204, Art 1

Skandinaviska Enskilda Banken AB (publ). SEB. (2007). Retrieved March 1, 2007, from www.seb.se

Smart technology solutions. (2006). A smart answer to online fraud? *Card technology today* (p. 10-11).

TeachTarget. (2007). *Biometrics* Retrieved February 27, 2007, from *http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci211666,00.html*

WDA.org (2007). *SSL,* Retrieved February 19, 2007, from *http://www.wda.org/Public/help/glossary.htm*

Appendix 1 – SE-Banken

Appendix 2 - Swedbank

Appendix 3 - Nordea

Appendix 4 - Nordea

Appendix 5 - Handelsbanken

Appendix 6 – Interview guide local banks (swe)

Vi är tre stycken studenter som kommer från Internationella handelshögskolan i Jönköping (Jibs) och skriver kandidat uppsats i informatik. Vår uppsats handlar om internet banker i Sverige. Därför skulle vi vilja intervjua ansvarig för er Internet bank.

Handledare

Jörgen Lindh P.hd inom informatik

Tel. 036-101780, mobil 070-7397395

Alla svar kommer att vara anonyma i vår rapport, vilket innebär att det inte kommer att tas upp vad ni specifikt svarar, utan svaren ska leda till någon form av generella drag.

Syftet är i stället att ta fram underlag för en analys som ska leda till generella principer vid beslut angående Internet banken Vilka faktorer som ligger till grund för valet av inloggningssätt samt vad man tror framtida inloggningssystem kommer att bli.

Frågor till lokala banker

1. Vilken funktion har ni?
2. Finns det någon ansvarig för tjänsten Internet bank?
   - lokalt?
   - huvudkontor?
3. Känner ni till på vilken nivå som beslut rörande tjänsten Internet bank tas?
4. Vet ni vilka som har det yttersta ansvaret för tjänsten Internet bank, som tar alla beslut rörande utveckling och användning av tjänsten?
5. Hur många arbetar med tjänsten Internet bank?
6. Hur mycket vet ni om nuvarande inloggnings system för tjänsten Internet bank?
7. Hur mycket vet ni om valet av inloggnings system, vilka faktorer som kan ha varit avgörande?
8. Vad vill ni ge för bild av tjänsten Internet bank gentemot era kunder?
9. Vet ni hur man hanterar incidenter angående tjänsten Internet bank?
   Om ja → ligger dessa på en acceptabel nivå?
10. Vet ni om inloggnings systemet som används idag kommer att förändras något den närmaste framtiden?

Appendix 7 – interview guide for local banks (eng)

Tutor: Jörgen Lindh P.hd within Informatics

Telephone nr: 036-101780, mobile 070-7397395

All the answers from this interview will be anonymous, which means that they will not be mentioned specifically instead the answers will lead to some form of general conclusion.

The purpose with this interview is to gather data for our analysis, in able to find out the fundamental choices behind the actual online banking access system and the aspect of future online banking access system.

Questions to the local banks

1. What position do you have in the bank?
2. Is anyone responsible for the service Internet Banking?
   -Local
   - central
3. At what level are the decisions made concerning the service Internet banking?
4. Is anyone outmost responsible for the service, which takes the overall decisions regarding development and use of the service online banking?
5. How many are currently working with the service Internet banking?
6. How much do you know about the current used online banking access system?
7. How much do you know about the choice of online banking access system, which factors has been the most conclusive?
8. What "picture" do you want to mediate to your customers?
9. Do you know how to manage incidents concerning the service?
   - If yes, do you feel these are in an acceptable level?
10. Do you know if the current used online banking access system will change in the future?

Appendix 8 – Interview guide for each banks HQ (swe)

Vi är tre stycken studenter som kommer från Internationella handelshögskolan i Jönköping (Jibs) och skriver kandidat uppsats i informatik. Vår uppsats handlar om internet banker i Sverige. Därför skulle vi vilja intervjua ansvarig för er Internet bank.

Handledare

Jörgen Lindh P.hd inom informatik

Tel. 036-101780, mobil 070-7397395

Alla svar kommer att vara anonyma i vår rapport, vilket innebär att det inte kommer att tas upp vad ni specifikt svarar, utan svaren ska leda till någon form av generella drag.

Syftet är i stället att ta fram underlag för en analys som ska leda till generella principer vid beslut angående Internet banken Vilka faktorer som ligger till grund för valet av inloggningssätt samt vad man tror framtida inloggningssystem kommer att bli.

Frågor till Huvudkontor

1. Vilken funktion har ni?
2. Hur många arbetar med tjänsten Internetbank?
3. Hur ser ni på utvecklingen av tjänsten Internetbank?
4. Beskriv ert nuvarande inloggningssystem?
5. Vem eller vilka utvecklar/utvecklade detta inloggnings sätt?
6. Vilka faktorer fick er att välja ert nuvarande inloggningssystem som ni använder idag?
7. Fanns det några grundläggande beslutsfattande faktorer till detta val?
    a. I sådana fall vilka är dessa besluts faktorer?
8. Hur hanterar ni incidenter?
9. Inom säkerhetsåtgärderna för er inloggning system, tror ni att dessa åtgärder kommer utvecklas i framtiden?
10. Om Ja hur tror ni att detta kommer att ske, och vilken påverkan kommer detta att ha på er verksamhet
11. Har ni funderingar kring hur ni kan höja trovärdigheten på autentieringen i framtiden?

Appendix 9 – Interview guide bank headquarters (eng)

Tutor: Jörgen Lindh P.hd within Informatics

Telephone nr: 036-101780, mobile 070-7397395

All the answers from this interview will be anonymous, which means that they will not be mentioned specifically instead the answers will lead to some form of general conclusion.

The purpose with this interview is to gather data for our analysis, in able to find out the fundamental choices behind the actual online banking access system and the aspect of future online banking access system.

Questions for the headquarters

1. What position do you have in the bank?
2. How many are currently working with the service Internet banking?
3. How do you look at the development of the service of Internet banking?
4. Describe your current online banking access system?
5. Who or whom develop/developed this online access system?
6. What factors made you choose your current online banking access system?
7. Are there any fundamental decision-based factors of the choice?
   - in this case what kind of decisions factors are there?
8. Do you know how to manage incidents?
9. Within the security measurements for your online banking access system, do you think these measurments will be developed in the future?
10. If yes, how will this be done and how will this affect your organization?

Do you have any thoughts about to increase the credibility of your authentication in the future?