Aalto University
School of Electrical Engineering
Degree Programme of Communications Engineering

Jussi Rämänen

Perceived security in mobile authentication

Master’s Thesis

Espoo, August 23, 2011

Supervisor:	Prof. Marko Nieminen, D.Sc. (Tech.)
Instructor:	Sirpa Riihiaho, Lic.Sc. (Tech.)

Aalto University
School of Electrical
Engineering

Aalto University School of Electrical Engineering Degree programme of Communications Engineering	ABSTRACT OF THE MASTER'S THESIS

Author: Jussi Rämänen

Title: Perceived security in mobile authentication

Number of pages: 8+108+7	Date: 23.8.2011	Language: English

Professorship: User Interfaces and Usability	Code: T-121

Supervisor: Prof. Marko Nieminen, D.Sc. (Tech.)

Instructor(s): Sirpa Riihiaho, Lic.Sc. (Tech.)

New advanced mobile phones and services enable users to handle a great number of tasks with their mobile phones, bringing increased flexibility. However, users have been reluctant to widely adopt the new mobile services. One of the most significant reasons for this are the security concerns of the users. Perceived security in mobile authentication has not been directly studied before, although it can be considered to have a great importance, as many of the new mobile services involve user authentication as an essential element. Therefore, this thesis aimed to form a good conception of this important topic.

The subject of perceived security in mobile authentication is approached through a literature review on the related research and an empirical study that was realized as a web survey. In the empirical study, both qualitative and quantitative data was collected, and it was carefully analyzed with proper tools. After analyzing the study results, a synthesis of the literature findings and the findings of the empirical study was performed.

The examination of this thesis revealed that perceived security is important for users and it considerably affects the intention to use mobile authentication. However, it was noticed that the effect significantly varies based on the service in question. A noteworthy observation was that half of the users are not using mobile banking services due to security concerns. In addition to generally determining the effect of perceived security on the use intention, this thesis identified factors that affect the formation of perceived security. A number of recommendations for taking perceived security into account in the design process were made based on the findings.

This thesis provides clear evidence that developing objectively secure authentication solutions does not alone guarantee user acceptance. The crucial factor affecting the users' intention to use mobile services is the subjective perception of security. Thereby, assuring users of the authentication security is of utmost importance. The thesis clearly highlights that perceived security is a complex concept and it is affected by various factors such as use context, service usage experience, and brand and reputation of service provider. This should be carefully considered when developing new mobile authentication solutions.

Keywords: perceived security, mobile services, authentication, user acceptance

Aalto-yliopisto
Sähkötekniikan korkeakoulu
Tietoliikennetekniikan tutkinto-ohjelma/koulutusohjelma

DIPLOMITYÖN
TIIVISTELMÄ

Tekijä: Jussi Rämänen

Työn nimi: Koettu turvallisuus matkapuhelimella tapahtuvassa tunnistautumisessa

Sivumäärä: 8+108+7

Päiväys: 23.8.2011

Julkaisukieli: englanti

Professuuri: Käyttöliittymät ja käytettävyys

Professuurikoodi: T-121

Työn valvoja: Prof. TkT Marko Nieminen

Työn ohjaaja(t): TkL Sirpa Riihiaho

Nykypäivän kehittyneet matkapuhelimet ja mobiilipalvelut tarjoavat käyttäjille joustavuutta mahdollistamalla monien tehtävien suorittamisen matkapuhelimella. Käyttäjät eivät kuitenkaan ole olleet laajasti halukkaita ottamaan käyttöön uusia mobiilipalveluja. Eräänä suurimmista syistä tähän on käyttäjien huoli käytön turvallisuudesta. Mobiilitunnistautumisen koettua turvallisuutta ei olla aikaisemmin suoraan tutkittu, vaikka sen merkitys on kiistaton tunnistautumisen kuuluessa olennaisena osana moniin uusiin mobiilipalveluihin. Tästä syystä tämän diplomityön tarkoituksena oli muodostaa käsitys koetusta turvallisuudesta mobiilitunnistautumisessa.

Koettuun turvallisuuteen perehdyttiin tässä diplomityössä sekä kirjallisuuskatsauksen avulla että kyselytutkimuksena toteutetun empiirisen tutkimuksen keinoin. Empiirisessä tutkimuksessa kerättiin sekä määrällistä että laadullista aineistoa, ja aineisto analysoitiin huolellisesti tarkoitukseen soveltuvia työkaluja hyödyntäen. Tulosten analyysiä seurasi kirjallisuuskatsauksesta nousseiden havaintojen ja empiirisen tutkimuksen tulosten rinnakkainen tarkastelu mahdollisten yhtäläisyyksien ja eroavaisuuksien tunnistamiseksi.

Tämän diplomityön löydökset osoittavat, että koetulla turvallisuudella on käyttäjille suuri merkitys ja se vaikuttaa merkittävästi aikomukseen käyttää mobiilitunnistautumista. Koetun turvallisuuden merkityksessä havaittiin kuitenkin selkeitä eroja palvelutyypistä riippuen. Merkittävää oli huomata, että puolet käyttäjistä ei käyttänyt pankkipalveluja matkapuhelimella turvallisuuteen liittyvistä huolista johtuen. Koetun turvallisuuden ja käyttöaikomuksen välisen yhteyden lisäksi diplomityössä selvitettiin myös tekijöitä, jotka vaikuttavat koetun turvallisuuden muodostumiseen. Diplomityön löydösten pohjalta laadittiin joukko suosituksia, joita noudattamalla koettu turvallisuus voidaan tehokkaasti huomioida suunnitteluprosessissa.

Tämä diplomityö osoittaa selkeästi, että objektiivisesti turvallisten tunnistautumisratkaisujen kehittäminen ei itsessään takaa käyttäjähyväksyntää. Käyttöaikomuksen kannalta olennaista on käyttäjän subjektiivisesti kokema turvallisuudentunne. Siksi käyttäjien vakuuttaminen tunnistautumisen turvallisuudesta on erittäin tärkeää. Diplomityö osoittaa, että koettu turvallisuus on monimutkainen käsite, jonka muodostumiseen vaikuttavat useat tekijät, kuten käyttökonteksti, käyttökokemus mobiilipalveluista sekä palveluntarjoajan brändi ja maine. Tämä on syytä huomioida kehitettäessä uusia ratkaisuja mobiilitunnistautumiseen.

Asiasanat: koettu turvallisuus, mobiilipalvelut, tunnistautuminen, käyttäjähyväksyntä

Foreword

I want to thank my supervisor Marko Nieminen as well as my instructor Sirpa Riihiaho for all of the valuable feedback I have received in the course of writing this thesis. I also want to thank Tapio Haanperä of the fruitful conversations related to the thesis and of his encouraging comments. Finally, I would like to say thanks to my family and friends from whom I have received energy during the process.

Otaniemi, 23.8.2011

Jussi Rämänen

Table of Contents

1 Introduction

In Asia and Europe, the adoption pace of new advanced mobile phones has been rapid, creating opportunities to develop a multitude of new mobile services (Mallat et al., 2004). In Finland, the distribution and penetration of mobile phones is among the highest in the world (approximately 7 million mobile subscriptions by 2008), which means that technical readiness for wide adoption of new mobile services exists (Bouwman et al., 2007; SVT, 2008).

Although many users have the possibility of using new mobile services, people have been hesitant in adopting the services. For example, there have been many attempts to popularize mobile payment services, but due to lack of wide user acceptance, the attempts have not succeeded for the most part. The reasons for failures include security concerns of users as well as lack of standardization, universality of the payment procedures, and incompatibilities with users' needs. Out of the determinants of service adoption, some authors have highlighted the lack of perceived security as being one of the most important reasons for refusal to use mobile payment services and mobile services in general. Therefore, improving users' security perceptions is essential in driving the growth of mobile service use. (Tsalgatidou & Pitoura, 2001; Jarvenpaa et al., 2003; Bauer et al., 2005b; Linck et al., 2006; Goeke & Pousttchi, 2010; Schierz et al., 2010)

Average users often do not understand the technical aspects of security correctly and are usually unable to evaluate the objective security (i.e. the technical security implementation) in the mobile services. Therefore, the user's subjective perception of security is the crucial factor to consider when developing new mobile services that users would use. (Salisbury et al., 2001; Bauer et al., 2005b; Linck et al., 2006)

Despite perceived security being identified as a critical factor for mobile service acceptance, research on the customers' security concerns and the concept of perceived security in general has been quite rare with respect to mobile applications. (Linck et al., 2006) As new mobile services are developed with an increasing pace, more research is needed to form a comprehensive conception of the factors that affect perceived security and how it can be improved.

This master's thesis was done within a Mobile Financial Services (MoFS, http://mofs.soberit.hut.fi/) research program funded by TEKES (the Finnish Funding Agency for Technology and Innovation). The aim of MoFS program is to promote the transition of financial services to the mobile environment, and to steer present use habits toward a "wallet in a mobile phone" mindset. The application domains in the program include trust services, payments, banking and ticketing. An interest towards developing a new, secure solution for mobile authentication existed within the MoFS program, and perceived security was identified as an important aspect that should be considered when designing the solution. As no previous research directly studying perceived security in mobile authentication existed, examining the subject was seen as a suitable topic for a master's thesis.

1.1 Scope of the thesis

This thesis explores perceived security in mobile services and particularly the user authentication in the services. Given the fact that the amount of perceived security research in mobile applications is still fairly low, the examination was extended to cover also thematically related research from the application areas of traditional computing. This was seen essential for making the literature review enough comprehensive.

Furthermore, it was noticed that considerable proportion of the related research deals with other constructs than perceived security. These constructs (i.e. perceived privacy, trust, perceived credibility and perceived risk) are, however, closely related to the construct of perceived security and are therefore included in the scope of this thesis.

As a great share of the related research builds around technology and user acceptance, including a brief introduction to this approach was considered to be important. Furthermore, perceived security, dealing with user's subjective perceptions, was seen as a topic also related to user experience, and therefore the concept of user experience is briefly covered. However, related research has not approached perceived security in the light of user experience, and neither has user experience research discussed the role of perceived security. Hence, user experience is not at the center stage of the examination of this thesis. The purpose of introducing user experience is to highlight the importance of taking perceived security as part of the user experience consideration, as many new mobile services involve handling of money and personal, sensitive information.

When the scope of the thesis was initially drafted, the plan was to include also a cognitive perspective to the topic. However, it became clear that it would not fit into the scope without expanding the thesis too much, and therefore the topic was excluded from the plan.

1.2 Objective and research questions

With a combination of a literature review on the related research and an empirical study this thesis aims at forming a comprehensive conception of the Finnish users' current attitudes and perceptions regarding security of mobile authentication, finding out possible differences in perceptions between mobile environment and traditional computing environment, discovering the factors that contribute to perceived security, as well as eliciting information of how the users' perception of authentication security could be improved. The objective is to provide developers of new mobile authentication solutions with useful information for considering perceived security when designing the solution, and thereby reducing the risk of introducing solutions that would not be accepted by the users.

This thesis aims to answer the following four research questions:

Rq1 How do Finnish mobile phone users currently perceive the security of mobile authentication?

A general conception of the current situation regarding Finnish users' attitudes and perceptions of mobile authentication security is important information to determine the need for actions in developing new solutions. However, no previous data of the present state exists, and therefore this information is to be acquired within this thesis.

Rq2 How does perceived security of mobile authentication differ from perceived security of authentication in regular web services?

Mobile Internet is still a relatively new phenomenon, and therefore many users do not have much experience of mobile services yet. This is assumed to make users more careful with mobile services than with regular web services therefore affecting perceived authentication security. The accuracy of this assumption is explored within this thesis.

Rq3 What factors affect perceived security of mobile authentication?

As perceived security is about users' subjective views and understanding, it is obvious that many factors contribute to the formation of perceived authentication security. This thesis aims to form a comprehensive picture of the different factors and their importance to perceived security.

Rq4 How to improve perceived security of mobile authentication?

To be capable of developing solutions that users perceive as secure, the designers and developers need information of what they should consider in the design process. This thesis aims to discover ways to improve perceived authentication security, and provide useful recommendations to address perceived security in the design of new authentication solutions as well as mobile services in general.

The research questions were mostly answered based on both the literature review and the empirical study. Table 1 clarifies the methods that were used for answering each of the research questions.

Table 1. Methods used for answering the research questions

Research question	Method
Rq1 Current situation	Empirical study
Rq2 Differences in perceived security between mobile and traditional computing environments	Empirical study + literature review
Rq3 Factors of perceived security	Empirical study + literature review
Rq4 Means to improve perceived security	Empirical study + literature review

1.3 Structure of the thesis

This thesis includes a literature review and an empirical study. Literature is covered in the Chapters 2 and 3, from which the Chapter 2 presents background information covering brief introductions to mobile services and mobile authentication, utilized security mechanisms in mobile environment, mobile use context, user experience, as well as technology acceptance. The purpose of Chapter 2 is to get the reader familiar with the essential background information of the thesis.

Chapter 3 presents literature review on the research conducted in the field of perceived security and other thematically related phenomena. The chapter covers a brief look at the research backgrounds, the terminology of the research domain, relationships between the different terms, factors affecting perceived security and other related constructs, as well as suggestion to improve perceived security and the other constructs.

The findings from the related research, together with the research questions that were set in the beginning of the thesis, served as a basis for designing the empirical study that is described in the Chapter 4. This chapter elaborates objective of the study, utilized methods and study design, as well as presents information of the study participants.

Chapter 5 presents the results of the empirical study. The results were structured and thoroughly analyzed using appropriate tools. The processed study results were finally synthesized with the findings from the related research (Chapter 3). The synthesis is presented in the Chapter 6.

Chapter 7 concludes the thesis by answering the research questions and presenting recommendations for considering perceived security when designing new mobile authentication solutions. Furthermore, Chapter 8 presents discussion related to the thesis.

Figure 1 illustrates the process of the thesis from literature review to synthesis.

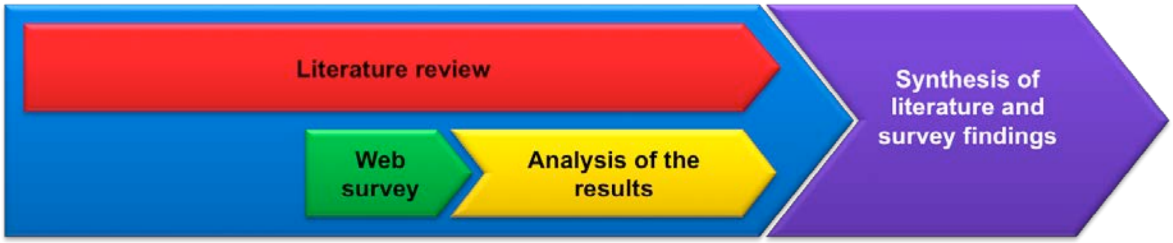


Figure 1. The process of the thesis

2 Background

Before exploring the related research of the thematic area of perceived security, it is worth presenting some background information of certain important topics. The purpose of background information is to orientate the reader to mobile application domain and environment as well as to present certain concepts that are later referred to in this thesis. Firstly, this chapter briefly provides general information of mobile services and the user authentication. Secondly, mobile use context and the differences it has to stationary context are explored. Thirdly, the chapter discusses user experience, and finally technology acceptance models that have been actively utilized in the related research of this thesis.

2.1 Mobile services and user authentication

As the topic of this thesis is perceived security in mobile authentication, it is essential to give certain information of what is meant by mobile services in general. By their nature, mobile services differ from regular electronic services with respect to the device, as mobile services are used with mobile devices such as mobile phones and other handheld or palm-sized computers (e.g. PDAs). To date, many of the services that were previously available only in the traditional computing environment have become available also as mobile services. These services include for example mobile shopping, mobile banking, email, content download (e.g. music and graphics), news, online games, stock trading, travel ticket booking and wireless coupons. Mobile ticketing and vending must also be highlighted along with social media services. Despite the active introduction of new mobile services, the consumers' interest towards using their mobile phone for service transactions is still relatively low. (Mallat et al., 2004; Wang et al., 2006; Kleijnen et al., 2007)

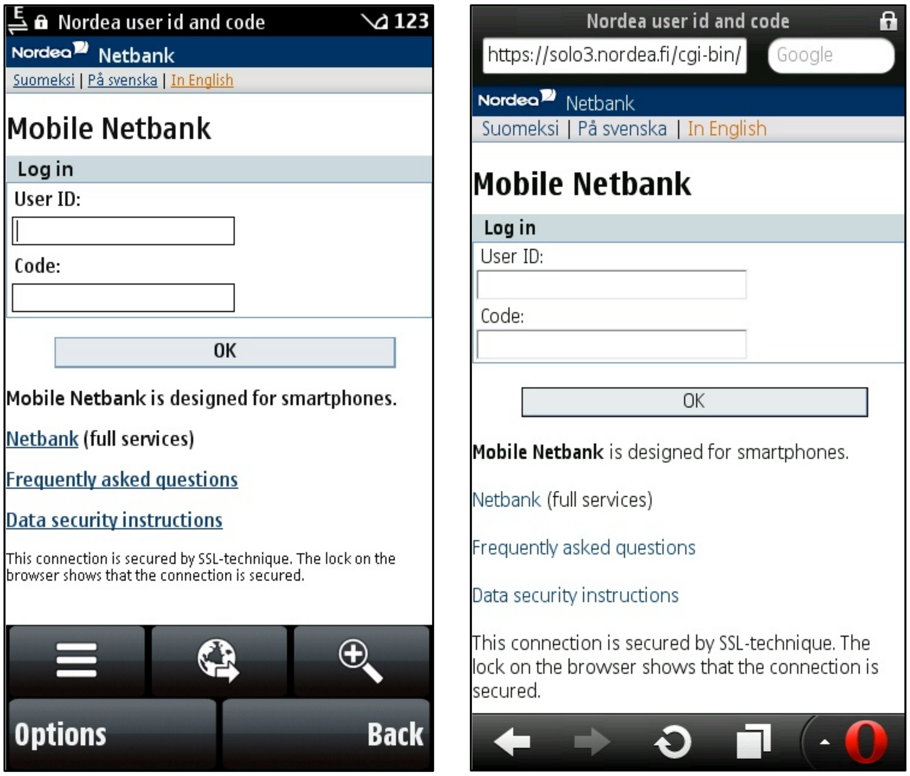
Compared to traditional wired electronic services, mobile services can be stated to bring additional values such as ubiquity, personalization and flexibility. Mobile services enable users to perform tasks irrespective of time and place, and they can also save effort in certain cases. User control can also be considered as one advantage of mobile transaction services. (Mallat et al., 2004; Wang et al., 2006; Kleijnen et al., 2007)

The nature of user authentication on mobile devices has not changed essentially since their introduction. Most of devices utilize point-of-entry protection via a Personal Identification

Number (PIN). In this regard, mobile devices and desktop systems share the same underlying principle of authentication approach that is based on secret knowledge. However, mobile devices differ from desktop system in one important respect that is the use of multiple mechanisms for locking different aspects of functionality. In the case of mobile phones, this means having separate protection mechanisms for the device and the user's SIM (Subscriber Identification Module). The fact that mobile phones utilize more than one protection mechanism can cause users confusion, and the confusion may be further increased by the varying styles of authentication codes. (Botha et al., 2009)

In addition to user authentication with respect to the protection of mobile device and user's SIM, there is also a great number of mobile services that involve user authentication one way or another, as user's confidential information is often required in the services, and it has to be protected for security reasons. Usually, confidential data is protected through use of encryption. In the traditional wired computing, PKI and TSL/SSL have been utilized as encryption techniques. For mobile services, wireless adaptions of PKI and TSL/SSL have been developed, and they have been standardized. (Mallat et al., 2004)

Figure 2 shows an example of a Finnish mobile banking service (by Nordea bank) that utilizes SSL encryption for handling the user's confidential authentication information. The left picture in the figure illustrates how the service appears when using the default browser of a Nokia 5800 XpressMusic smart phone (with a touchscreen). The other picture on the right side shows the view of the same service, but with Opera Mini mobile browser (a popular alternative browser). As can be seen from the Figure 2, both of the browsers show an indication of encrypted connection with a lock icon located in either of the top corners. Additionally, the service provider has provided written message of the SLL encryption at the bottom of the view.


Nordea user id and code
123
Nordea Netbank
Suomeksi | På svenska | In English
Options
Back
Nordea user id and code
https://solo3.nordea.fi/cgi-bin/
Google
Nordea Netbank
Suomeksi | På svenska | In English
OK

Mobile Netbank

Log in

User ID:

Code:

OK

Mobile Netbank is designed for smartphones.

Netbank (full services)

Frequently asked questions

Data security instructions

This connection is secured by SSL-technique. The lock on the browser shows that the connection is secured.

Mobile Netbank

Log in

User ID:

Code:

Mobile Netbank is designed for smartphones.

Netbank (full services)

Frequently asked questions

Data security instructions

This connection is secured by SSL-technique. The lock on the browser shows that the connection is secured.

Figure 2. Examples of encrypted mobile service authentication

Some researchers have highlighted that use of mobile services involves more security risks compared to the traditional Internet services in the desktop environment. Chari et al. (2001) state that mobile usage entails new security risks compared to desktop environment. These risks originate from underlying technology differences and increased pervasiveness. Problems arise, for example, from the technological limitations of mobile devices, and the increased portability also increases the likelihood of theft, loss and damage. Also Gruen (2006) expresses that most mobile devices have a relatively weak wireless communication security, although the technology is advancing. The more advanced ones of the mobile devices support for example public-key encryption, but there are many other devices that do not have great encryption capabilities. Furthermore, a more recent research by Botha et al. (2009) claims that the level of security protection in mobile devices is not at the same level as in desktop systems, although mobile devices store an increasing amount of sensitive data and enable access to many of the same services and application as desktop systems.

2.2 Mobile use context

As this thesis explores perceived security particularly in mobile context, it is important to understand how this context differs from other more stationary contexts. This subchapter elaborates characteristics of mobile devices, usability challenges in mobile use, and the mobile use context.

2.2.1 Mobile devices

According to Gorlenko and Merrick (2003) a device is fully mobile when both user and device can be in motion during the use. Being fully mobile also requires that the device can be used without placing it on any surface. Hence, for example laptop computer is not fully mobile but only transportable. Besides mobile phones and other handheld devices, Gorlenko and Merrick (2003) also mention that fully mobile device can be something user is wearing such as a wrist computer. Weiss (2002) has also defined three qualities a handheld fully mobile device must possess. Firstly, it has to be easily used while held in hands. Secondly, the device should operate without cables with exceptions of recharging and synchronizing. Lastly, there has to be either possibility of installing new applications or support for Internet connection.

2.2.2 Challenges of mobile usability

Gorlenko and Merrick (2003) divide the usability challenges of mobile device use into three groups, namely technical, environmental and social challenges. Technical challenges are related to network connectivity issues, security hazards, and device design constraints such as small screen and limited battery life. Environmental challenges, in turn, involve issues like variation in temperature and lightning conditions, noises and distractions, mobility of the user, subdivision of user’s attention between multiple tasks, and physical restrictions. The authors highlight the fact that while the technological challenges can be resolved due to technological development, the environmental challenges cannot be reduced significantly. The third group of challenges, the social challenges, includes personalization, comfort, acceptance and adoption issues as well as privacy concerns, particularly in applications based on location-awareness.

Botha et al. (2009) highlight an aspect of authentication with mobile phone that may cause frustration for the users. Mobile use is much more ad hoc by its nature than desktop use, so users may not use the phone for a long period at a time but may, instead, quickly want to check, for example, a schedule entry. Thus, a scenario where unlocking the device takes more time than the actual task is possible if the user has enabled the device lock in the phone. This can cause users frustration and may lead to a situation where users do not utilize authentication for the sake of convenience. (Botha et al., 2009) Some studies have, indeed, revealed that authentication is used less on mobile devices than on the desktop system and inconvenience has been mentioned as one reason for this behavior (Clarke & Furnell, 2005; Karatzouni et al., 2007).

2.2.3 Mobile use context

Gorlenko and Merrick (2003) discuss mobile interaction by dividing it into two contexts: mobile office context and field context. In mobile office context, mobile devices are used as complementary means for stationary computers to carry out traditional office computing tasks. In field context, on the other hand, only fully mobile devices are utilized for carrying out both professional and non-professional activities, and traditional computing is not involved. The interaction characteristics of the two contexts have been elaborated based on eight interaction parameters: environment, device size, time of interaction, user mobility, competition for attention, task hierarchy, parallel manipulation of physical objects outside interaction and interaction styles. The authors have also compared the mobile contexts to stationary context.

1) **Environment.** In the case of both mobile interaction contexts environment varies frequently between indoors and outdoors, whereas stationary interaction happens mostly indoors and there is little variability in the environment.
2) **Device size.** In both mobile contexts, device size is small, while stationary interaction involves use of medium to large sized devices.
3) **Time of interaction.** The time that user is involved in the user-device interaction varies from short to medium in the case of mobile interaction, and from medium to long in stationary interaction.
4) **User mobility.** Mobile and stationary contexts differ in user mobility. Mobile interaction allows users to be in any position and free body movement is possible. Stationary interaction, instead, requires fixed position and the freedom of action is

very limited.

5) **Competition for attention.** Stationary interaction involves only little subdivision of user’s attention. Mobile office context involves a little more competition for attention than stationary context. In the case of field context, the competition for user’s attention is significant.

6) **Task hierarchy.** This interaction parameter denotes the relation of interaction to other activities user is involved in. In the case of stationary interaction, interaction-related tasks are generally the user’s primary activity. In mobile office context, interaction tasks may be secondary activity, and in the field context, interaction tasks are mostly secondary activity.

7) **Parallel handling of objects during interaction.** Handling of objects during interaction is rare in stationary interaction, occasional in mobile office context, and frequent in field context.

8) **Interaction styles.** This parameter describes the way interaction is happening or should happen in different contexts. Stationary interaction is mostly based on direct manipulation and other interaction styles are complimentary. In mobile office context, the use of forms and menu selection is of major importance, and in addition to direct manipulation also possibility to utilize natural language should be provided. In field context, the use of natural language should be of prime importance with forms and menu selection supplementing it. Gorlenko & Merrick (2003) suggest that interaction in the field context should be as flexible as possible, and therefore user should be able to choose which interaction style is most suitable in any given situation.

In their study about use contexts of mobile Internet Kim et al. (2005) state that mobile context consists of any personal or environmental factors that can affect the user while using mobile Internet. Therefore they divided mobile context into personal and environmental contexts. These two sub-contexts are also broken further down so that personal context involves internal context referring to user’s goals and emotions, and external context referring to the way user is using hands and legs. Environmental context, in turn, is divided into physical context consisting of visual and auditory distractions, and social context meaning user’s location relative to other people and the level of external interaction. In the studies the authors found out that the use of mobile Internet was strongly concentrated around two key contexts. This finding contradicts with general beliefs according to which mobile Internet would be used in diverse contexts. Although very flexible use is possible, people seem to favor only a few contexts. In the most frequent use context users have a hedonic goal, they feel joyful, device is used with one hand, their legs are static, visual and auditory distractions are low, user is not surrounded by many people, and their interaction with others is low. The second most frequent context is identical to the first context except for the goal that in this case is utilitarian instead of hedonic. The findings of Kim et al. (2005) suggest that mobile Internet would be used in office or home-like contexts rather than outdoor and moving contexts.

2.3 User experience

Perceived security is determined by user's subjective evaluation of the service. Therefore, it is also a matter of user's experience of the service. However, perceived security has not been connected to user experience in the literature, although a clear connection exists. This subchapter gives a brief overview of user experience as a topic by presenting some of the popular definitions.

For a relatively long period of time, studies have been conducted in the field of usability by several researchers. Lately, researchers have started to increasingly talk about user experience or UX, being a more holistic concept covering not just the pragmatic aspects of product possession and use, but aiming at the balance between the pragmatic and other non-task related aspects (Hassenzahl et al., 2006). Although user experience has now been studied for a fairly long time, and common agreement of the definition has been achieved to some extent, researchers still have different approaches to the topic originating from their backgrounds and research interests (Law et al., 2009). This makes it difficult to ensure that people are talking about the same subject as they use the term user experience. Next, some definitions for UX will be presented to illustrate the different viewpoints of the researchers and to highlight the elements UX have been stated to enclose.

One of the latest definitions for user experience is presented in the new standard definition for user experience (ISO 9241-210:2010). Getting a standardized definition for the term can be considered as an indication of at least some sort of agreement regarding the subject. In the standard (ISO 9241-210:2010) user experience is defined as *“person's perceptions and responses resulting from the use and/or anticipated use of a product, system or service”*. This relatively abstract definition doesn’t give detailed information of what user experience actually is. However, the definition has been further elaborated in three notes that help in the interpretation of the definition. The first note states that “u*ser experience includes all the users' emotions, beliefs, preferences, perceptions, physical and psychological responses, behaviors and accomplishments that occur before, during and after use*.” This note highlights the various mental aspects the use of a product involves, and also expresses the time dimension of the use, i.e. the experience is also affected by the periods before and after the actual use. The second note adds to the first note by highlighting also the product related aspects of user experience and the context of use: *“user experience is a consequence of brand image, presentation, functionality, system performance, interactive behavior and assistive capabilities of the interactive system, the user's internal and physical state resulting from prior experiences, attitudes, skills and personality, and the context of use.”* The third note concludes by stating that *“usability, when interpreted from the perspective of the users' personal goals, can include the kind of perceptual and emotional aspects typically associated with user experience. Usability criteria can be used to assess aspects of user experience.”* This note can be seen as a link between usability and user experience helping to see the connection between the two concepts.

Although a standard definition for user experience now exists, the construct also has other relevant definitions that originate from the different backgrounds and interests of the researchers in the field. Marc Hassenzahl is one of the pioneers in the UX research. Since the early 2000s he has been doing active research around the topic, exploring the user-product relationship from the basis of pragmatic and hedonic attributes as the determinants for the product’s appealingness and the resulting pleasure and satisfaction. (Hassenzahl; 2001, 2003, 2006) According to his definition user experience is *“a consequence of a user’s internal state (predispositions, expectations, needs, motivation, mood etc.), the characteristics of the designed system (e.g. complexity, purpose, usability, functionality etc.), and the context (or the environment) within which the interaction occurs (e.g. organizational/social setting, meaningfulness of the activity, voluntariness of use etc.)”* (Hassenzahl & Tractinsky, 2006). This definition has been widely recognized and has gained popularity (Law et al., 2009). Hassenzahl (2010) has also presented a newer definition presenting that user experience or experience in general can be defined based on four key characteristics. According to the definition, experience is subjective, holistic, situated and dynamic. By subjectiveness, Hassenzahl means that objectively similar situations can result in completely different experiences. The second attribute, holistic, refers to Hassenzahl's three level hierarchy of goals, proposing that besides the lower level "do goals" and "motor goals" telling what is done and how, there would also be so-called "be goals" that reflect why something is done, thus creating a personal meaning for the activities. Situated means that experience is always linked to a specific situation that makes it unique. However, Hassenzahl states that there can be similarities between the experiences and thus experiences can be categorized. The fourth attribute, dynamic, means that the experience usually changes when the time passes. Hassenzahl makes also an important remark that the design should cause positive emotions in the user. By this point, Hassenzahl differentiates user experience from usability that is often though as a matter of identifying and removing problems and barriers. (Hassenzahl, 2010)

Peter Morville (2004), a well-known researcher in the field of information architecture and the Web, approaches user experience through a UX Honeycomb framework (see Figure 3, right). The framework consists of seven attributes that, in his opinion, determine user experience. Additionally, Morville uses the three circles of information architecture (see Figure 3, left) as a broader framework in which he discusses his UX Honeycomb. This framework has not only been used by Morville, but also many other researchers as well as the new ISO 9241-210 standard (2010).

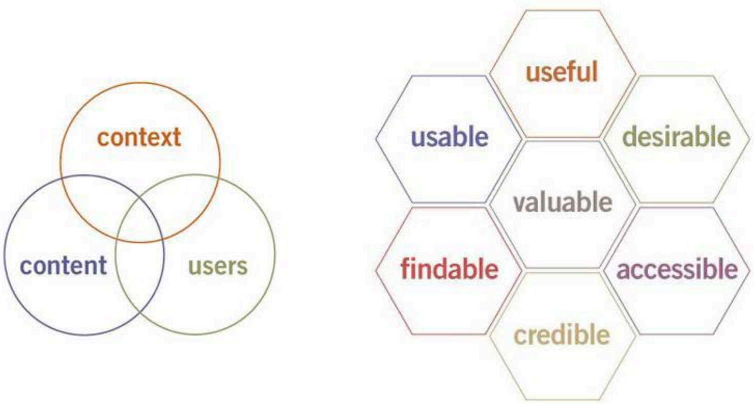


Figure 3. UX Honeycomb framework by Morville (2004)

The UX Honeycomb by Morville visually highlights certain characteristics or determinants of UX. One of the elements in the honeycomb, credibility, is thematically closely related to this thesis. This might give an interesting starting point to start building the missing relationship between user experience and perceived security.

2.4 Technology acceptance models

Technology Acceptance Model (TAM) that was introduced by Davis in 1986 is the most popular and common theory that has been used to describe user acceptance of information technology (Davis et al., 1989; Chau & Hu, 2001; Goeke & Pousttchi, 2010). It can be viewed as the most influential model to extend the theory of reasoned action (TRA) and the theory of planned behavior (TPB) (Ajzen & Fishbein, 1980; Ajzen, 1985; Bagozzi, 2007). TAM is based on the idea that two particular beliefs, perceived usefulness and perceived ease-of-use, are of primary importance in determining computer acceptance behaviors (Davis et al., 1989). The model is illustrated in Figure 4.

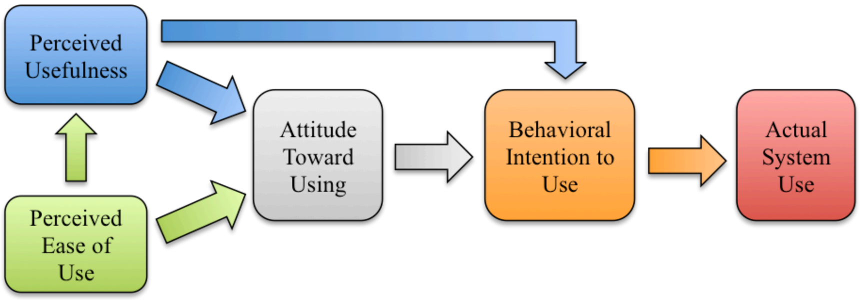


Figure 4. Visualization of TAM (Davis et al., 1989)

Perceived usefulness is defined as *“the prospective user's subjective probability that using a specific application system will increase his or her job performance within an organizational context”* and perceived ease of use, on the other hand, refers to *“the degree to which the prospective user expects the target system to be free of effort”* (Davis et al., 1989). As figure 2 shows, both perceived usefulness and perceived ease of use affect the attitude toward using a system, and added to this, perceived ease of use also affects perceived usefulness. The behavioral intention to use is jointly determined by the user’s attitude toward using a system and perceived usefulness, and the intention to use determines the actual usage behavior. (Davis et al., 1989) Some researchers have simplified TAM model by removing the attitude construct (Venkatesh et al., 2003).

Despite its great influence, TAM has also been criticized. Bagozzi (2007) states that while the simplicity of TAM can be considered its main strength, it is also a great challenge, as explaining a wide variety of things precisely with a very simple model possesses great difficulties. TAM was originally intended for studying the user acceptance of information systems in business context where users do not, for example, voluntarily take new systems into use, but are enforced to do so by the organization (Kaasinen, 2005). To make the TAM model better applicable also to other contexts outside business, some extensions to the model have been presented. TAM2 model by Venkatesh and Davis (2000) is one of these, expanding the original TAM model by specifying factors that affect perceived usefulness and intention to use, as well as introducing the influence of experience and voluntariness. A great share of the related research of this thesis has approached perceived security and the other related constructs by utilizing TAM model as the basis for research framework. TAM2 serves as a good example of how TAM model have been expanded. It is visualized in Figure 5.

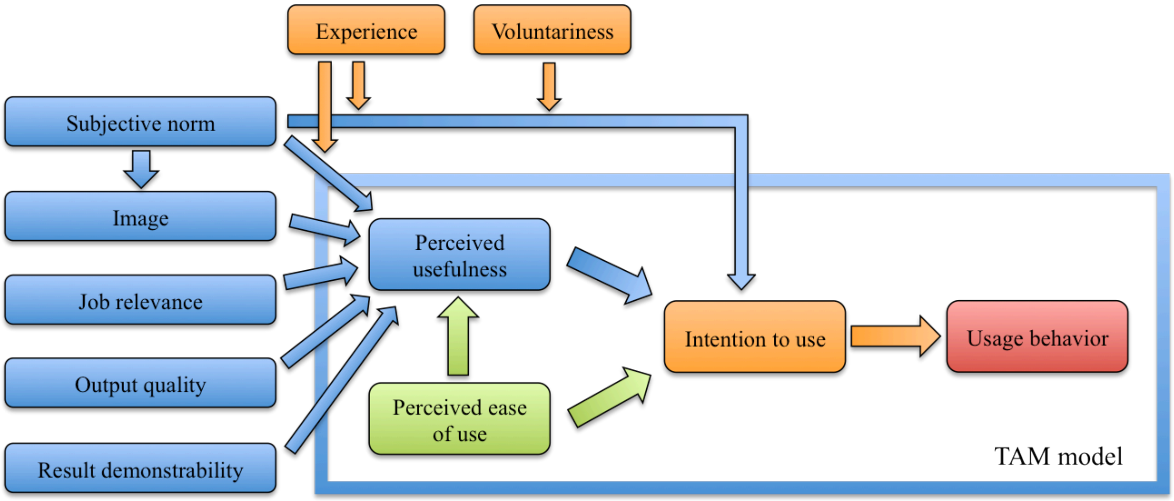


Figure 5. TAM2 model

Kaasinen (2005) has presented a technology acceptance model for mobile services (TAMM) that is based on the original TAM model but has been slightly modified and complemented with elements that make it better suitable for mobile context (see Figure 6).

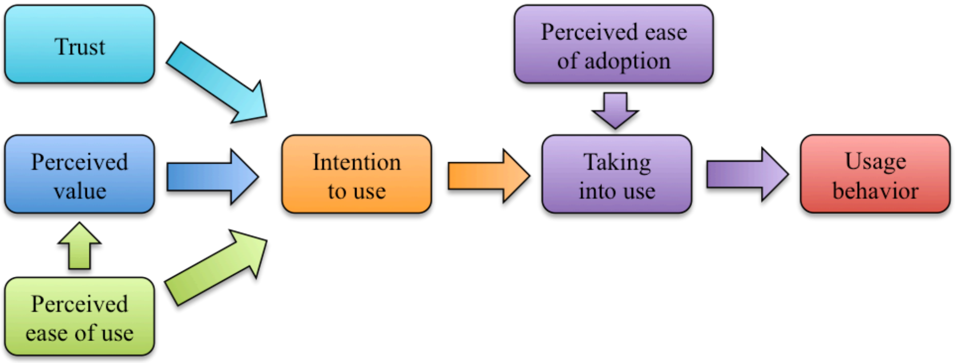


Figure 6. TAMM model

When comparing this model to the original TAM model, it can be noticed that perceived usefulness has been replaced with perceived value. According to Kaasinen (2005), perceived usefulness may not indicate sufficient motivation for the users to acquire a mobile service, when considering consumer products. Value, instead, includes not only rational utility but also other aspects of the product that the users appreciate and are interested in a new product. Kaasinen (2005) has extended the original TAM model by adding trust as one factor affecting intention to use. In the business context, for which the Davis's (1989) TAM model was developed, the users can rely on the safety of services as they are brought to them by the organization. In the case of consumer services and particularly the complex mobile service networks, on the other hand, trust in the service providers becomes an essential aspect. Trust in the TAMM model includes perceived reliability of the technology and the service provider, reliance on the service in planned usage situations, and the user's confidence that the service is under his/her control and that his/her personal data will not be misused by the service. Besides trust, the TAMM model also includes the phase of taking the service into use, which is located after use intention, before the actual usage behavior. Kaasinen (2005) suggests that this phase is affected by perceived ease of adoption. Similarly to trust, taking the services into use is not an issue in business context, as the applications are installed for the users. Consumer services, however, require user's effort when a new service is taken into use, and troubles at the adoption stage can considerably affect whether the user will end up using the service or not. The TAMM model does not incorporate characteristics of the user and his/her social environment that affect the perception of service. However, Kaasinen (2005) admits that these are aspects that should be taken into consideration.

Although various extensions to the TAM model have been presented, Bagozzi (2007) claims that they have only broadened the model by introducing new predicting factors of either perceived usefulness or intention to use. He states that very few research cases have attempted to deepen TAM by expanding on perceived usefulness and perceived ease-of-use, forming new conceptualizations of the variables in the model, or proposing new variables that would explain the effects of the existing variables.

3 Related research

This chapter explores the literature from the thematic area of this thesis. As the related research involves use of multiple concepts and terms, the examination of this thesis covers the concepts of perceived security, perceived privacy, trust, perceived credibility and perceived risk. Firstly, the chapter briefly discusses the backgrounds of the studies that have been involved in the examination of the related research. Secondly, definitions that related research has suggested for the key constructs of this thesis, followed by an explanation of the relationships between the constructs is presented. Furthermore, the chapter explores the factors that contribute to the formation of the construct in the thesis' scope. Also the effects of the constructs to user acceptance are examined. Finally, the chapter presents some recommendations that authors in related research have suggested to improve users' perception of security.

3.1 Research backgrounds

The researches that were explored for the related literature part of this thesis originate from various application areas. Many of researches relevant to this thesis have not been carried out in the mobile application areas, as research related to mobile services is still relatively new. However, the studies from other application areas were included in the thesis because of the fairly low number of studies related to mobile application area. Figure 7 illustrates the application areas from which researches were included in the literature review of related research. Most of the studies were either from the application area of electronic commerce (e.g. Jarvenpaa et al., 2000; Miyazaki & Fernandez, 2001; Gefen et al., 2003; Vijayasarathy, 2004) or Internet banking (e.g. Wang et al., 2003; Pikkarainen et al., 2004). The studies incorporated into this thesis do not directly explore perceived security in mobile authentication, as there is no such research available. Nevertheless, majority of the studies are from application areas that involve user authentication as one element of the service (e.g. banking and commerce).

A great number of the studies of this chapter approach perceived security from the perspective of user acceptance and they are mostly theoretically based on technology acceptance model (e.g. Hsu & Chiu, 2004; Gu et al., 2009; Schierz et al., 2010; Goeke & Pousttchi, 2010). TAM model has been used as a starting point when building the research framework, and certain constructs have been added to the original model by the authors as they have empirically tested the effects of some factors to user acceptance.

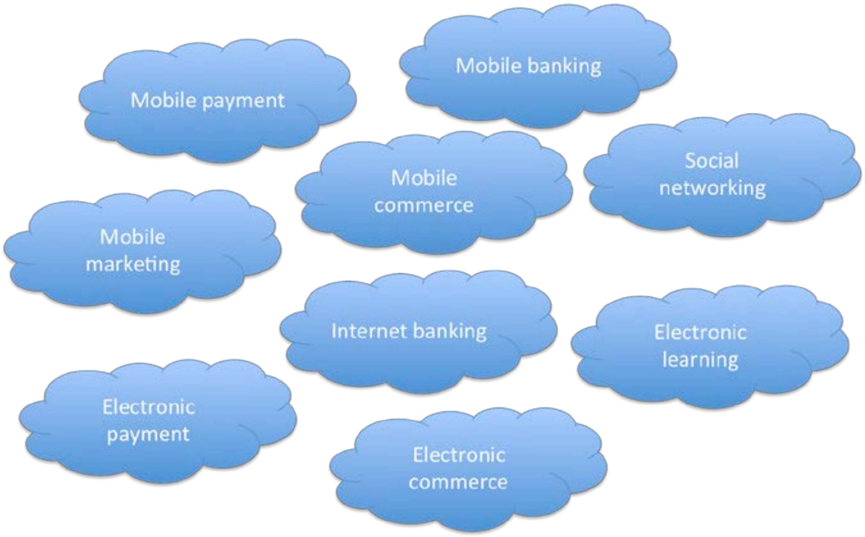


Figure 7. Application areas of the related research

The methodology utilized in the studies was in many of the cases similar. The most typical procedure was to collect the data through a pretested questionnaire, and usually the questionnaires consisted of Likert-type statements (e.g. Gefen et al., 2003; Ong et al., 2004; Vijayasarathy, 2004; Kim et al., 2010; Schierz et al., 2010). Also other methods such as experiemental tasks (e.g. Jarvenpaa et al., 2000) and telephone interviews (Wang et al., 2003) were utilized by some reserachers.

3.2 Terminology

The research that is thematically connected to this thesis, involves use of several terms, all of which are related to the same entity, but approach it from slightly different angles. Therefore, it is essential to define and explore these terms, so that the reader will be able to differentiate between them in the following chapters of this thesis. The terms to be defined are perceived security, perceived privacy, trust, perceived credibility and perceived risk.

3.2.1 Perceived security

Perceived security can be defined in different ways depending on the detail level and sophistication that authors want to convey. Vijayasarathy (2004) has taken a simple and straightforward approach by defining perceived security as *“the extent to which a consumer* *believes that making payments online is secure"*. The definitions of Yenisey et al. (2005) and Shin (2010) are analogous to the definition of Vijayasarathy (2004). Casaló et al. (2007), on the other hand, define perceived security in more detail as a two-dimensional construct including the users' perception of the conventions of handling personal data protection in the financial services web site, and the security of the information system in which these conventions take place.

Linck et al. (2006) present a division of the concept security into objective and subjective security in their study concerning security issues in mobile payment. Objective security is determined by five security objectives, namely confidentiality, authentication, integrity, authorization and non-repudiation. Confidentiality refers to securing the transaction information from unauthorized persons. Encryption is generally used for this purpose. Authentication, in turn, is defined as the means to verify that the transaction information originates from the correct transaction partner. An identifier such as a PIN code or a biometric property can be utilized in the authentication procedure. The third security objective, integrity, is about preserving the transaction information unaltered during transmission. The fourth objective, authorization, is about being able to verify that parties involved are permitted to perform the transaction. Finally, the last objective, non-repudiation, refers to protection against fraudulent unauthorized transactions using someone else's identity. Digital signatures are utilized to fulfill the objectives of integrity and non-repudiation, whereas digital certificates are utilized for authorization.

Linck et al. (2006) use a term subjective security as a synonym for perceived security and define it as "the degree of the perceived sensation of the procedures' security from the viewpoint of the customer". Pousttchi and Wiedemann (2007), in turn, state that subjective security is "the degree to which a person believes that using a particular mobile payment procedure would be secure".

3.2.2 Perceived privacy

Although privacy matters are not the main focus of this thesis, it is still essential to define the term to avoid possible misunderstandings of the terminology. Wang et al. (2003) define privacy as the protection of all the data that is collected (with or without users being aware of it) during users' interactions with an Internet banking system. Perceived privacy can therefore be defined as the user’s perception of aforementioned. Shin (2010) suggests that privacy would be a subset of security, and defines privacy as the *“control over the flow of one’s personal information, including the transfer and exchange of that information”*.

Casaló et al. (2007) Casaló et al. (2007) remark that the concepts of privacy and security often tend to be mixed up and used as synonyms, although they clearly have different meanings. The authors state that privacy refers to certain legal requirements and good practices regarding the handling of personal data, whereas security is about the technical guarantees that ensure that the legal requirements and good practices regarding privacy will be effectively fulfilled in practice. Despite highlighting that distinction of the concepts, Casaló et al. (2007) express that consumers, companies and the legislator perceive the concepts as being closely related, and therefore the authors present the concepts of security and privacy as being part of the single construct of perceived security in the handling of private data. They define the construct as the consumer’s perception of the personal data protection practices and the security of the system where the practices are to be found.

3.2.3 Trust

Trust has been studied in many contexts and there are a variety of definitions for it. Baier (1986) has defined trust as *“accepted vulnerability to another’s possible but not expected ill will (or lack of good will) toward one”*. Also other authors have used the term vulnerability in their definitions for trust. According to Corritore et al. (2003), for example, trust means one party’s (i.e., trustor) belief that the other party (i.e., trustee) involved in a relationship will not exploit its vulnerability. Shin (2010), in turn, defines trust as one party’s willingness to be vulnerable to the actions of another party, while the other party is performing actions that one cannot monitor and control.

Shneiderman (2000) approaches the concept of trust from the perspective of future expectations and thus defines trust as “the positive expectation a person has for another person or an organization based on past performance and truthful guarantees”. Also Ba & Pavlou (2002) use expectations in their definition, according to which trust is *“the subjective assessment of one party that another party will perform a particular transaction according to his or her confident expectations, in an environment characterized by uncertainty”*. This definition takes into account also the context in which the trusting relationship takes place.

Casaló et al. (2007), in turn, see trust in a wider sense as they present it as a construct consisting of three dimensions, namely honesty, benevolence and competence. By honesty they refer to the belief that the other party will be sincere and keep their promises. Benevolence, in turn, reflects the belief that interest on each other's well-being exists. Competence represents consumer's perceptions of the seller's ability to complete a relationship and satisfy consumer's needs.

In marketing literature, trust has been inspected as a twofold construct that involves benevolence and credibility as dimensions (Doney & Cannon, 1997; Ganesan, 1994). Ba & Pavlou (2002) have summarized the definitions from marketing literature and characterize benevolence as the belief that one party is genuinely interested in the other party's welfare and has intentions and motives that are beneficial to the other party even under unfavorable conditions that have not been included in the commitment. Credibility, on the other hand, the authors see as the belief that the other party will demonstrate honesty, reliability and competence in the relationship.

3.2.4 Perceived credibility

The construct of perceived credibility has been used in many researches thematically close to this thesis and is closely connected to the concept of trust. Therefore it is essential to define and elaborate the term here. Different definitions can be found from different sources, with slightly different approach angles and varying level of detail.

Ong et al. (2004) give perceived credibility a simple definition that they state is limited in terms of breadth, but is one way to approach the construct. The authors define perceived credibility as the degree to which a user thinks that using a certain system is free of privacy and security threats. Also Wang et al. (2003) see perceived credibility in a similar manner. Ba & Pavlou (2002) describe perceived credibility as being impersonal and depending on reputation, available information and economic reasoning.

3.2.5 Perceived risk

Perceived risk is also one of the constructs that have been utilized in the research related to this thesis. Wang et al. (2003) define it as the user's subjective expectation of suffering a loss when pursuing a desired outcome. Wu & Wang (2005) approach perceived risk as a multi-dimensional construct that covers certain financial, product performance, social, psychological, physical, or time risks that can be involved in an online transaction.

Perceived risk can also be approached based on two types of uncertainty, namely behavioral uncertainty and environmental uncertainty. Behavioral uncertainty refers to the risks that result from the fact that web retailers have the possibility to behave opportunistically and exploit the distant and impersonal nature of online commerce. Environmental uncertainty, on the other hand, involves technology-driven risks and the fact that Internet possesses unpredictability and is therefore in control of neither the web retailer nor the consumer. (Pavlou, 2003)

3.3 Interconnections between the constructs

Some of the authors in the related research have pointed out connections between some of the constructs that were presented in the Chapter 3.2. These interconnections are highlighted in this subchapter.

Perceived security → trust. Shin (2010) claims that perceived security moderates the effects of perceived privacy and trust. Enhanced feeling of security is stated to improve the perception of trust, and there is a significant relationship between the two concepts. Perceived privacy is claimed to have effect on trust through perceived security and therefore it can be considered as the mediating effect. However, the effect of privacy is not as significant as the effect of security. Shin (2010) considers perceived security and perceived privacy as antecedents of trust. Kim et al. (2008) refers to perceived security protection and perceived privacy protection as cognition-based trust antecedents and states that both of them have a strong, positive effect on trust. Casaló et al. (2007) present that perceived security in the handling of private data has a positive and significant effect on the consumer trust in an online banking web site.

Shin (2010) states, unlike other studies, that the effect between perceived security and trust would be two-way. He also shows that although both the effect of trust into security and security into trust are significant, the effect of security into trust is stronger of the two. Goeke & Pousttchi (2010), on the other hand, present that only trust affects perceived security significantly.

Perceived security → perceived risk. Related literature shows that there is also a connection between perceived security and perceived risk. The findings of Kim et al. (2008) suggest that the consumers' perceptions of security protection and privacy protection both strongly influence perceived risk in online shopping, by reducing it. The results of the authors also indicate that consumers seem to independently value privacy and security.

Trust → perceived risk. A connection between trust and perceived risk has also been presented in the literature. Based on their findings, Kim et al. (2008) suggest that consumer’s trust significantly reduces the consumer’s perceived risk. Also Jarvenpaa et al. (2000) have presented that trust significantly decreases perceived risk. Furthermore, Pavlou (2003) has identified trust is an important factor decreasing perceived risk.

3.4 Determinants of the constructs

This subchapter gives a brief introduction of how people in general perceive security as well as explores the factors that, according to the related research, affect perceived security and privacy, trust, perceived credibility and perceived risk.

According to West (2008) there are certain principles of human behavior that determine the way people think about security. He claims that people subconsciously think that they are less likely to be affected by computer vulnerabilities than others, and this leads to underestimation of security risks. He also suggests that people increase risky behavior as they have security elements such as firewalls in use. West (2008) mentions that, due to limited capacity for information processing, people might not be able to consider all risks, consequences and alternatives.

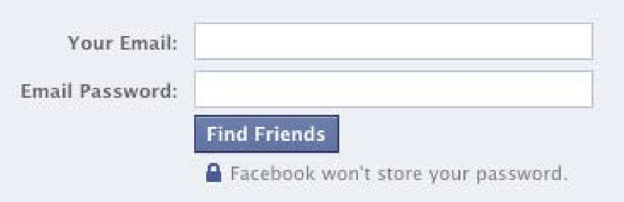
West (2008) states that in order to understand perceptions of security and decision-making, it is important to notice that safety is an abstract concept. An example illustrating this is the fact that when we take care of security, the reward is that nothing unwanted happens. In other words, there is no such thing as a concrete reward for being more secure. West (2008) argues that people do not perceive gains and losses equally, and therefore he states that in any given moment of decision user must perceive greater magnitude of gain than of loss because otherwise loss would be more motivating in the decision.

One of West’s (2008) important notions is that security is usually a secondary task for users. Usually people have to make security decisions while they are carrying out some task. They often want to get the primary task done as quickly as possible and thus are likely to make decisions that will lead to as few interrupts as possible. This kind of behavior might result in security risks.

Perceived ease-of-use and usability. The study of Linck et al. (2006) identified convenience and ease-of-use as important factors positively affecting perceived security. The positive, significant effect of ease-of-use on perceived credibility has also been confirmed in various studies. For example, Wang et al. (2003) and Ong et al. (2004) have presented this relationship to hold in the case of electronic services. A positive, significant effect of perceived ease-of-use on trust has also been presented by some authors (e.g. Gefen et al., 2003). Furthermore, Casaló et al. (2007) state that usability directly and significantly affect users’ trust in a web site dealing with financial services. The authors also state that usability positively affects perceived security by improving comprehension of the tasks and content and making users feel more comfortable. Gefen et al. (2003) have also highlighted that an interface that complies with common conventions and situational norms is likely to increase trust of the users. Also Gu et al. (2009) have stated that situational normality positively affects trust.

Provided security information. Botha et al. (2009) state that Internet browsers in mobile phones are much more limited in terms of user-configurable security and privacy options than browsers in desktop systems. The authors argue that, although mobile browsers do dot support many of the features that are likely to introduce security risks (e.g. ActiveX), the users are not well informed about the differences in vulnerability between mobile and desktop contexts, and therefore the lack of security options can have negative effects on the security experience.

Security statements. Providing the user with assuring statements of how security is being taken care of in the service and the level of security with utilized security procedures has been indicated as a factor that positively affects both perceived security and trust. The positive effect on trust is presented, for example, in the study by Mukherjee & Nath (2003). Lim (2008), in turn, point out that informing and assuring the users of the security positively influences both the trust and the perception of security. Kim et al. (2010) have also expressed the favorable effect of security statements on perceived security in their study. In the study of Linck et al. (2006) security statements were ranked among the most important factors that affect perceived security. An example of security statement is shown in Figure 8.



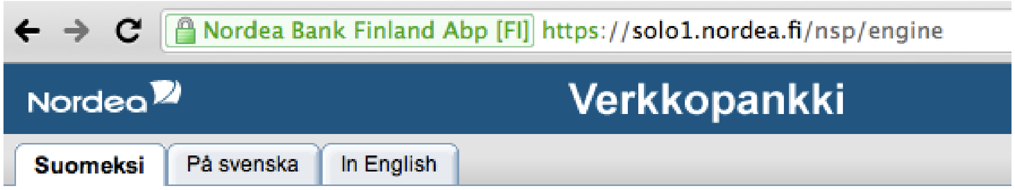
Facebook won't store your password.

Figure 8. An example of security statement ("Facebook won't store your password.")[1]

Information quality. The significance of information quality of the service content can be found from the related research. Kim et al. (2008) have presented that information quality, which they consider as a cognition-based trust antecedent, has a strong, positive effect on trust.

Perception of security mechanisms. It has been confirmed that users pay attention to security mechanisms that are utilized in the services, and that they have effect on users' perceptions of security. Linck et al. (2006) have presented that the level of objective security influences the level of subjective security. Their study confirmed a significant positive effect of encrypted connection to perceived security. The effect of encrypted connection has also been reported by Pousttchi & Wiedemann (2007). Kim et al. (2010) have claimed that user's perception of the technical protection in the service affects perceived security strongly and positively, and the authors also present that technical protection significantly and positively affects trust. Furthermore, Gefen et al. (2003) have expressed that user's perception of the safety mechanisms utilized in the service affects trust significantly. An example of how encrypted connection is indicated in Google Chrome Internet browser is shown in Figure 9.

[1] http://www.facebook.com

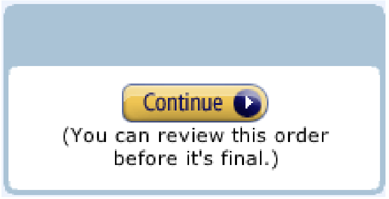


Nordea Bank Finland Abp [FI] https://solo1.nordea.fi/nsp/engine
Nordea
Verkkopankki
Suomeksi
På svenska
In English

Figure 9. An example of encryption indications (lock sign and https prefix) in the case of Nordea Internet bank website[2] and Google Chrome Internet browser[3]

Technology self-efficacy and user expertise. Some researches have presented a relationship of computer self-efficacy (i.e. user's perception of his/her ability to use computer to accomplish certain tasks) to perceived credibility. Both Wang et al. (2003) and Ong et al. (2004) confirmed a significant negative effect of self-efficacy in their studies, indicating that increasing technological ability and awareness would make the users increasingly suspicious. However, the total effect of computer self-efficacy on behavioral intention to use via perceived credibility was still positive in both studies. Laforet & Li (2005) have presented that past experience with computer and new technology significantly and positively affect the service adoption. Bauer et al. (2005a), in turn, have stated that lack of previous experience of new products or services is likely to cause higher perceived risk. Also Shin (2010) has suggested that user expertise may affect the perceptions of security and privacy.

Uncertainty of action consequences. Bauer et al. (2005a) have stated that uncertainty about the consequences of a decision or an action leads to increase in perception of riskiness. Figure 10 shows an example from the Amazon.com purchasing procedure of how the user can be informed about the consequence of action.



(You can review this order before it's final.)

Figure 10. An example of how user can be informed of the consequence of action[4]

[2] https://solo1.nordea.fi/nsp/engine
[3] http://www.google.com/chrome

Amount of payment. Goeke & Pousttchi (2010) state that payment amount does not generally have influence on perceived security, and neither to general security aspects such as privacy, anonymity and traceability. However, the authors note that payment amount does have effect in the cases of authorization and confirmation. Bauer et al. (2005b) state that in the case of larger amounts, the users' main concern is the security of the payment. The users' main fear, according to the authors, is that an unauthorized third party would intercept the transaction process and copy, delete or alter data. Because of the security concerns, users are willing to accept more complex and slower transaction procedures. On the other hand, Bauer et al. (2005b) highlight that in the case of smaller amounts users prefer easy and fast procedures and are more willing to accept lower security level. Also Mallat et al. (2004) state that users seem to be willing to use fairly simple authorization mechanisms (e.g. telephone number or personal identification number) in the case of micropayments. Coursaris & Hassanein (2002) also makes an important remark by stating that consumers are not likely to purchase very expensive items online, and they are even more hesitant toward purchasing with mobile phone.

Mismatch between perceived security and actual security. Yenisey et al. (2005) argue that users' perception of security can differ significantly from the actual security level on an e-commerce site. A site with well-implemented security may not show users clear indications of it, and on the other hand, a site with very bad security implementation may give users misleading impressions of good security. Shin (2010) also highlights that, at least in social networking, there is a possibility that users perceive security incorrectly as they associate third party content with a web site they trust.

The type of the service. According to Coursaris & Hassanein (2002) users become increasingly concerned of the safety of the information transferred over a wireless network as the degree of interaction and the sensitivity of the exchanged information increases. Thus, the authors claim that security of less personal and interactive services such as weather notifications does not bother users, whereas services involving more interaction and personal information (e.g. mobile banking) concern users more. Some authors (e.g. Gefen et al., 2003; Mitchell, 1999) have stated that users often perceive services riskier than

[4] http://www.amazon.co.uk/

products because they are, for example, intangible and more vacillating, which makes them challenging to evaluate.

The effect of device. Coursaris & Hassanein (2002) state that minimal security mechanisms in mobile devices cause users security concerns as data is increasingly being transferred over mobile networks. In the case of mobile devices, there also exists a greater opportunity for abuse and misuse due to the nature of mobile use (Varadharajan, 2000).

It has been stated that mobile devices are by their nature more vulnerable to security threats such as theft or accidental loss than computers that are used in fixed locations. Therefore, identification and authentication need to be specifically considered. Moreover, the level of security protection in mobile devices is not at the same level as in desktop systems, although mobile devices store an increasing amount of sensitive data and enable access to many of the same services and application as desktop systems. (Bauer et al., 2005b; Botha et al., 2009)

In their studies about security and trust in mobile interactions, Kindberg et al. (2004) discovered that many users instinctively considered docked, physical connections more secure than wireless connections. However, the users were not able to clearly explain their opinion but expressed a general concern toward the insecurities of the wireless link. Kindberg et al. (2004) also noticed that something being close or local is considered more trustworthy. Thus, it seems that boundaries increase perceived security to some extent, perhaps by making the situation appear more controllable for the user. Based on this assumption mobile connections, due to its nature, would be perceived less secure than physical connections.

Reliability. Coursaris & Hassanein (2002) highlight the importance of maintaining connection quality in mobile networks. Breakdowns of connection can cause concerns of the personal data being lost. Losing critical information during financial transaction, for example, can have serious consequences, which can increase users’ concerns. Also Linck et al. (2006) have identified technical reliability as a factor contributing to perceived security.

The effect of experiences. Miyazaki and Fernandez (2001) discovered that consumers with positive previous experiences in online shopping are likely to continue making online purchases in the future. The authors state that the perceptions of privacy and security risks decline as the amount of positive experiences increases. Also Pavlou (2003) got results showing that positive experiences both decrease perceived risk as well as increase trust. Furthermore, Lim (2008) has suggested that users' satisfaction originating from favorable experiences is likely to affect trust positively.

Familiarity. According to Ba & Pavlou (2002) one factor to affect the formation of trust is familiarity and repeated interaction. The authors note that familiarity takes time to build up and is therefore not involved when a new service is introduced to users. Also Kim et al. (2008) have presented that familiarity, which they call an experience-oriented trust antecedent, significantly increases trust.

Consumer disposition to trust. Kim et al. (2008) have stated that consumer disposition to trust, which they characterize as a personality-oriented trust antecedent, significantly increases trust. The authors state that consumer's disposition to trust refers to the consumer's general propensity to show faith in humanity and to adopt a trusting attitude towards other people. They claim that varying dispositions to trust originate from different developmental experiences, personality types and cultural backgrounds.

Perceived incentives for cheating. The user's subjective evaluation of the costs and benefits of cheating to the other party has been indicated as a factor that affects trust. An increase in trust is gained if the user estimates that the other party has no good incentives for cheating, and on the other hand, mistrust can increase if the other party can gain large profits by cheating. (Ba & Pavlou, 2002; Gefen et al., 2003; Gu et al., 2009)

Institutional structures. Ba & Pavlou (2002) state that institutional structures that promote confidence in goodwill and trustworthy behavior of a service provider positively affect trust. It is, however, noted by the authors that institutional structures in the online environment are not quite developed yet.

Perceived size of the actor. Doney & Cannon (1997) state that perception of large organizational size indicates that other consumers trust the organization and have done business successfully with it, and hence strengthens the consumer's trust that the organization will deliver on its promises. Large size can also be considered as a signal that the company should have the necessary expertise and resources to arrange support systems such as customer and technical services. The existence of these systems has a positive effect on trust. (Chow & Holden, 1997) In addition, Jarvenpaa et al. (2000) state that large actors have invested more resources in their business and are therefore perceived to have more to lose than small companies when behaving in an untrustworthy manner. In their studies, Jarvenpaa et al. (2000) confirmed that perceived size affects trust positively. They also found out that perceived size affects trust differently in different cases: when the possible loss in the case of fraud is significant, perceived size seems to have more effect than in a case where the possible loss is considered to be small.

Third-party seal. Linck et al. (2006) have identified third-party certification as a factor contributing to the formation of perceived security. Also Kim et al. (2008) have stated that the use of third-party seal, which they consider as an affect-based trust antecedent, reduces the risk perceived by the user. Figure 11 shows three examples of third-party seal indications from web services.

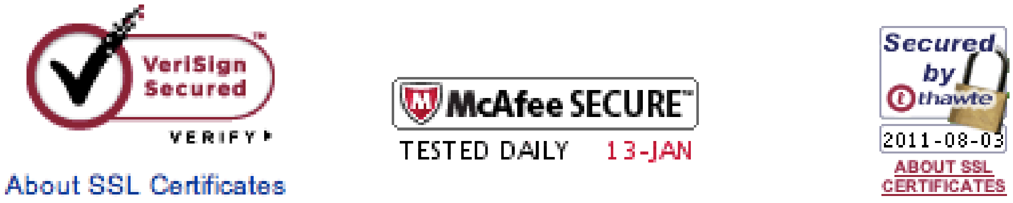


Figure 11. Examples of third-party seals (from left: eBay[5], Solgar[6], OnlineSolutions[7])

Reputation. Reputation has been stated to be an important factor that significantly affects both trust and perceived risk (Doney & Cannon, 1997; Zucker, 1986; Kim et al., 2008), the effect being positive in case of trust and negative in case of perceived risk. Also other authors have expressed the important role of reputation when users assess the trustworthiness of a service provider and the riskiness involved (e.g. Jarvenpaa et al., 2000; Ba & Pavlou, 2002; Pavlou, 2003; Casaló et al., 2007). Jarvenpaa et al. (1999) claim that reputation has a more significant effect on trust than perceived size does.

User demographics. The effect of users' demographics has been mentioned in the related research. Shin (2010) states that the gender, geographical location and culture of the user

[5] https://signin.ebay.co.uk/
[6] http://www.solgar.co.uk/
[7] http://www.solutions.fi/content/fi/11501/1206/1206.html

can affect the perceptions of security and privacy. However, he did not examine the effects of these factors in his study.

3.5 Perceived security and the related constructs as part of user acceptance

A great number of research cases related to perceived security, trust and other related constructs have been theoretically based on user acceptance. Consumer acceptance has also often been used as a synonym for user acceptance. Typically, the developed frameworks derive from the TAM model of Davis et al. (1989). In these researches based on extended TAM, perceived security and the related constructs have not been recognized for long. The researches have been divided into two groups: one examining the effect on use intention through the attitude toward use and the other examining the direct effect. The following two subchapters explore these two different approaches.

3.5.1 The direct effect on use intention

Miyazaki & Fernandez (2001) state that perceived system security is the most significant factor affecting the online shopping intention. The inconveniences of online shopping were also found to concern users significantly The results of Salisbury et al. (2001) also indicate that security is a remarkable determinant of the purchase intention, and it is claimed to have more influence than, for example, the ease and utility of purchasing products. Shin (2010) suggests that perceived security has a very strong effect on the intention to use social networking services.

A direct effect of trust on use intention has been presented in a number of studies (e.g. Pavlou, 2003; Gefen et al., 2003; Liu et al., 2005; Casaló et al., 2007; Kim et al., 2008, Gu et al., 2009). The studies have presented that trust significantly and positively affects the use intention. Kim et al. (2008) have even claimed that trust is the strongest predictor of the online consumer’s purchase intention followed by perceived benefit and perceived risk. Mallat (2007) has divided trust into trust in merchants, trust in telecom operators and trust in financial institutions, and all of these are proposed to have positive effect on adoption of mobile payments.

Some authors have included perceived credibility as a construct in their research frameworks that are based on the TAM model. Wang et al. (2003) explored the effect of perceived credibility on the intention to use Internet banking and got results showing a significant positive effect on the behavioral intention to use. Also Ong et al. (2004) studied the same relationship in the context of electronic learning (e-learning) and found a positive effect on use intention. In addition, Ong et al. (2004) stated that perceived credibility seems to influence users' attitudes toward using a service.

Some studies have also confirmed a relationship between perceived risk and the intention to use. Jarvenpaa et al. (2000) state based on their study results that perceived risk has a significant, negative effect on use intention. Also other authors (Pavlou, 2003; Kim et al., 2008) have presented similar findings. Furthermore, Mallat (2007) has divided perceived security risks into unauthorized use, transaction errors, lack of transaction record and documentation, vague transactions, concerns on device and network reliability, and concerns on privacy. She states that all of these factors have negative effect on mobile payment adoption.

3.5.2 The effect on use intention through the attitude toward use

Vijayasarathy (2004) studied the effects of perceived security and privacy on use intention through the attitude toward use. His results indicated a positive and significant effect of perceived security on the attitude, as well as a significant effect of attitude on use intention. Similar findings have been presented by Shin (2010). The hypothesis of positive effect of perceived privacy on the attitude in the study of Vijayasarathy (2004) was not supported. Laforet & Li (2005) have stated that consumers' attitudes are significantly affected by perceived security, and that attitudes have an important role in the service adoption. Also Schierz et al. (2010) have discovered an indirect influence of perceived security to use intention. Based on their research results they claim that perceived security has a significant effect on the attitude towards using mobile payment services, which in turn significantly affects intention to use. However, the authors highlight that the effect in their study was not as strong as some other researches have suggested, and hence the security concerns would not have a central role in the consumer acceptance of mobile payment services. Perceived compatibility was found to have the greatest impact on the intention to use mobile payment services, indicating that the services have to fit the existing behavioral patterns of users.

There have been studies that have shown a connection between trust and use intention through attitude. Jarvenpaa et al. (2000) found out a significant, positive effect of trust on attitude as well as a significant, positive effect of attitude on the use intention.

Hsu & Chiu (2004) tested for the effect of perceived risk on the attitude toward using an electronic service (e-service) and got results supporting their hypothesis of perceived risk level negatively affecting the attitude. Attitude toward using was also confirmed to affect the use intention. Also Jarvenpaa et al. (2000) have presented similar findings of the effects between perceived risk and attitude as well as attitude and use intention. Hsu & Chiu (2004) state that perceived risk plays an important role in affecting the users' decisions to adopt e-services, and it should not be overlooked. Furthermore, Laforet & Li (2005) have stated that consumers' attitudes are significantly affected by perceived risk, and that negative attitudes can be obstacles to service adoption. Also Bauer et al. (2005a) examined the effect of perceived risk on the attitude toward mobile marketing and got results that confirmed the hypothesized negative effect of perceived risk on attitude.

3.5.3 No effect or little effect on use intention

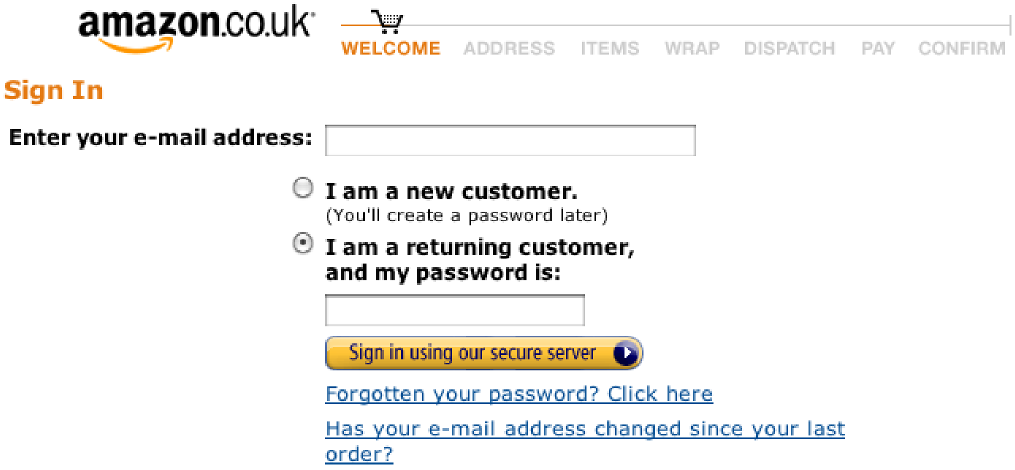
Although a great number of studies have presented use intention is affected by perceived security and the related constructs, a few authors have presented opposite statements. Goeke & Pousttchi (2010) claim that neither trust nor perceived security have effect on the intention to use mobile payment. Also Pikkarainen et al. (2004) state that security and privacy do not seem to statistically affect use intention in online banking context. Goeke & Pousttchi (2010) argue that in qualitative studies about mobile payment, users consider security as one of the most important aspects but quantitative studies have suggested that security does not actually have significant effect on use intention. This makes the authors assume that security is important for the users, but it is a basic need and therefore it does not affect the acceptance of mobile payment. Similar conclusions were made also in an earlier study of Pousttchi & Wiedemann (2007). It should be noted that some of the studies presenting significant effects of perceived security and the related constructs on use intention are actually quantitative studies (e.g. Shin, 2010), which is contradictory to the statements of Goeke & Pousttchi (2010) and Pousttchi & Wiedemann (2007).

There have also been less extreme statements about the insignificance of perceived security and the related constructs. Kindberg et al. (2004) identified three different user types in the context of mobile interactions: trust-oriented, convenience-oriented and socially oriented. The majority of the study participants did not express clear concerns related trust and security. Instead, the importance of convenience was emphasized in the study.

3.6 Designing for improved perceived security and trust

This subchapter presents certain suggestions that some authors have made to improve perceived security. Some of the guidelines are somewhat specific to a certain application area. In addition to the suggestions presented here, a number of other suggestions can be formed based on the factors identified in the Chapter 3.4.

Provide assuring information to the users. According to Salisbury et al. (2001) perceived security can be enhanced by showing information messages about the actions taken to safeguard against fraud every time the user is asked to enter sensitive information. An example of this can be found from Amazon website (see Figure 12).



Sign In

Enter your e-mail address:

○ I am a new customer.
(You'll create a password later)

● I am a returning customer, and my password is:

Forgotten your password? Click here

Has your e-mail address changed since your last order?

Figure 12. An example of assuring information message ("Sign in using out secure server")[8]

Provide feedback. Casaló et al. (2007) suggest that perceived security could be supported by providing the users with proper feedback so that users would feel they are better in control of what they are doing and where they are.

Provide evidence of past performance. It has been suggested by Shneiderman (2000) that

[8] https://www.amazon.co.uk/

service provider should make evidence of past performance available for the users. This can mean for example showing numbers of sold items in the last month.

Provide evidence of the company size. Jarvenpaa et al. (2000) has presented a significant effect of perceived size on trust, and therefore recommends that companies should utilize this fact by, for example, visibly stating the large size to the users in the service (e.g. “the world’s largest music store”), as well as providing the user evidence of large size by showing numbers of physical locations or the company staff.

Provide references from other users. To improve trust, Shneiderman (2000) also encourages providing references from past and current users in the service. This can be done for example by showing citations of positive customer feedback on the web site. The key idea is openness, as sharing information openly is claimed to enhance trust by mitigating suspicions. Also Jarvenpaa et al., 2000 highlight that showing quotes of customer satisfaction policies and customer testimonials regarding the quality and value of the service can be an effective way to boost the reputation perceived by users.

Provide guaranteed protection. One suggestion that Shneiderman (2000) has made on how to support trust is to provide guaranteed protection against credit card fraud and to promise customers a compensation for delayed delivery or other shortcomings in the service. Bauer et al. (2005b), in turn, suggest that in order to increase trust in the case of payments that are processed with mobile phone, user should be provided with reimbursement guarantees. They also present that the reversal of the payment transaction should be possible.

Provide comprehensible information of the terms and conditions and the service provider. Related to users’ need to have information available, Stroborn et al. (2004) suggest that users should be provided with clear presentation of the terms and conditions of the service as well as comprehensive information about the service provider. Furthermore, Shneiderman (2000) highlights that the privacy and security policies should be made easy to locate and comprehensible for the users.

Clarify responsibilities. Shneiderman (2000) have presented a guideline suggesting that, in order to enhance users’ trust, the service provider should clearly and comprehensibly clarify the responsibilities and obligations of each participant in the relationship.

Design intuitive user interfaces. Androulidakis et al. (2010) point out that regardless of users caring about security issues, they are not well aware of the actions they should take to avoid the security risks related to the mobile phone usage. That is why the authors suggest that better user interfaces should be designed to help the users to mitigate the security risks. Shneiderman (2000) has highlighted good design as a means to enhance users' trust. He suggests that attention should be paid to the structure of the web site as well as the intelligibility of the content and transaction processes. Bauer et al. (2005b), in turn, suggest that to increase trust of payments with mobile phone, the payment procedure should be easy to handle.

Invest in branding. The use of brand names, especially existing brands of banks, is a reasonable means to address security concerns, such as trust in mobile payment service provider. According to Shneiderman (2000), branding process builds trust by the use the familiar logos and respected company names. Yenisey et al. (2005) claim that brand name recognition and the reputation of the company are essential aspects of trustworthiness in online shopping context. Amazon is mentioned as an example of a company that benefits greatly from its good reputation as a safe online store. Also Casaló et al. (2007) highlight the importance of managing the corporate image, and this way affect the reputation. Promoting web sites by emphasizing the advantages and the offered services, as well as conveying a message of the concern with the consumer's well-being are presented as examples for enhancing the reputation. Linck et al. (2006) also mention informative advertising as one way to increase users' knowledge and thereby lessen the security concerns.

Utilize third party companies. Bauer et al. (2005b) suggest that trusted third party actors and trust-intermediates may be effective in reducing perceived riskiness of mobile applications. Also Goeke & Pousttchi (2010) state that trust can be improved by being proved by an independent institution. Shneiderman (2000), in turn, suggests the use of certifications from third parties such as TRUSTe to build customer trust. According to the findings of Jarvenpaa et al. (2000), in turn, reputation is also an essential factor in building trust, especially when the company is not large in size and cannot therefore utilize perceived size as a means to increase trust. As means to utilize the positive effect of reputation on trust, the authors recommend collaboration with companies that have an established, excellent customer reputation, and as a sign of collaboration having logos or names of these companies visible in the service. Jarvenpaa et al. (1999) mention seals of approval by third parties as an example of this. An example of how an independent organization can be utilized as a proof of trustworthiness is shown in Figure 13.

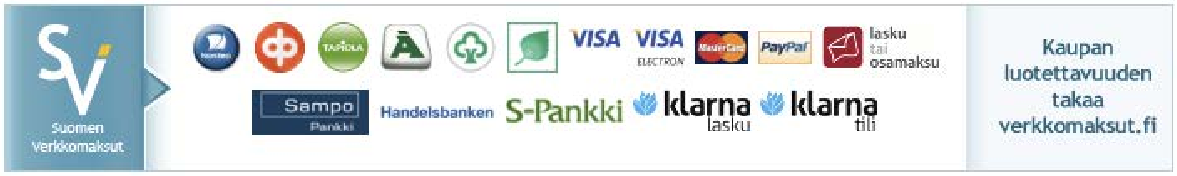


Figure 13. An example of having an independent organization as a proof of trustworthiness[9]

Invest in customer service. Shneiderman (2000) has highlighted the importance of good customer service for trust. He states that taking good account of the customer service procedures concerning dispute resolution is very important, as handling unsatisfied customers correctly is very important for maintaining trust.

Increase users' online expertise. Miyazaki and Fernandez (2001) believe that the increasing level of consumers' online expertise will help to mitigate the perceived security and privacy risks.

[9] http://docs.verkkomaksut.fi/api-index/

4 Empirical work

This chapter presents a description of the empirical study of this thesis. First, the objective of the study is presented. Then, the procedure of the study is explained. Thirdly, the chapter describes the methods utilized in the study and how they were applied. Finally, the last subchapter provides information about the study participants.

4.1 Objective of the study

The aim of the empirical study of this thesis was to gather comprehensive data about the users' views regarding perceived security of authentication that could then, together with the literature findings from related research, be used for thoroughly answering the research questions that were set in the beginning of the process.

The first objective of the study was to form an overall conception of the Finnish users' attitudes and security perceptions regarding mobile authentication, users' security awareness, and the visibility of security to users. The second objective was to identify factors that contribute to the formation of users' security perceptions. Thirdly, the study aimed at pursuing ideas on how the perceived security of mobile authentication solutions could be improved as well as exploring users' attitudes towards a new kind of mobile authentication solution.

As it was assumed that not all of the study participants would have experience of mobile authentication, the study also had an additional objective of collecting material of the perceived authentication security in regular web services used in the traditional computing environment, and based on this information comparing the differences between mobile and traditional computing environments.

4.2 Methods

This subchapter presents the methods that were utilized in the empirical part of this thesis. Firstly, the method that was used for gathering the empirical data (i.e. web survey) and the way it was utilized in the study are explained. Secondly, the chapter presents the tools that were used for analyzing the collected data.

4.2.1 Web survey

The data for the empirical part of the thesis was collected with a web survey. A survey was considered as a reasonable way to collect a wide variety of opinions in a relatively short time period. With a combination of closed and open-ended questions, the survey was seen as a suitable method for gathering both high-level quantitative data as well as more specific and profound qualitative data about the users' reasoning.

The survey was realized with the Forms tool of Google Docs web service[10], which was considered to suit the purpose. In the course of a few weeks, a total of 79 people (university students) completed the survey. The survey was carried out in collaboration with another thesis worker Tapio Haanperä and thereby it consisted of two parts. Approximately half of the survey consisted of questions regarding perceived security, the topic of this thesis, whereas the other half consisted of questions related to person-to-person mobile payment. Two versions of the survey were made, one with perceived security questions first, followed by questions regarding person-to-person mobile payment, and the other version with a reversed question arrangement. This was seen as an essential procedure for the survey design, helping to mitigate the bias caused by the order of the two different question sets. The last number of the participants' student number determined which one of the two survey versions the participant would take, so that participants with even number took one version and the ones with odd number took the other. This way it was possible to divide the participants in two groups of almost equal size. The survey contained a total of 49 questions, out of which 26 were related to the topic of this thesis. The survey involved both open-ended questions and questions with response alternatives. The distribution between the question types was even. The questions of the web survey are presented in the Appendix A.

In the web survey, brief definitions for the used terms and concepts were provided for the respondents before answering the questions. The purpose of this procedure was to reduce confusion caused by uncommon terminology and to get all the respondents to answer the questions as they were intended. Mobile service was defined as any web-based service used with a mobile phone and requiring the user to enter personal identification data or other

[10] http://www.google.com/google-d-s/forms

personal information. Facebook, email services, online bank and electronic commerce services were mentioned as mobile service examples. The provided definition for authentication was that user is asked to enter personal identification information such as username, password, personal identification number (PIN) or credit card number, when he/she is logging in to a service or performing certain actions in a service.

4.2.2 Data analysis tools

During the empirical part of this thesis, both quantitative and qualitative data was collected. Microsoft Office Excel was utilized for processing the raw quantitative survey data in order to determine the response distributions of the survey questions and to produce graphical illustrations of the results. Furthermore, a statistical tool called StatPac Statistics Calculator[11] was utilized in determining the statistical significance of the findings. It is an intuitive tool that enables getting reliable information of the significance of the results fast and conveniently. An important reason for selecting StatPac Statistics Calculator as the tool was that it enabled easy calculation of statistical significances for percentual proportions. The tool is only available for Windows environment.

In the analysis of the qualitative results, a tool called TAMSAnalyzer[12] was used for categorizing and structuring the collected data. The tool enabled identification of central themes and phenomena from the material and also enabled getting some quantitative data out of the open-ended survey questions. TAMSAnalyzer is a text analysis markup system that helps in analyzing qualitative data as the researcher can identify themes in texts such as web pages, interviews or field notes. The tool was initially designed for use in ethnographic and discourse research.

4.3 Study design

The study was designed in a top-down manner, first exploring general facts to form an overall conception of the characteristics of the study participants as well as their views on certain central matters, and then deepening the examination by enquiring more specific information. The study started by collecting background information that could be utilized when analyzing the gathered data. This information included demographical data of the

[11] http://www.statpac.com/statistics-calculator/index.htm
[12] http://tamsys.sourceforge.net/

study participants as well as the use habits of the users. The rest of the study concentrated on fulfilling the set study objectives (Chapter 4.1), starting with general perceptions, then more specifically exploring the effects of certain factors on perceived security, and finally enquiring both ideas on how perceived security could be improved and attitudes towards a new way to handle mobile authentication.

The study was designed in such way that responding was possible for both the respondents who had experience of mobile authentication and the participants who had not used mobile services that require authentication. The latter group of respondents was instructed to complete the study based on their authentication experiences of regular web services used with a computer.

4.4 Study participants

Altogether, 79 people participated in the web survey. All of the study participants were students from a bachelor-level basic course on user-centered product development (T-121.3110 – Käyttäjäkeskeisen tuotekehityksen harjoitustyöt[13]). Completing the web survey was a mandatory part of the course. Majority of the respondents (72 of 79 respondents, 91%) were bachelor’s degree students. The presented facts show that the study participants formed a relatively homogenous group in terms of background.

Based on the responses to a few demographic questions it was possible to find certain differences among the participants. Majority of the respondents (56 of 79 respondents, 71%) were men. This can be explained by the fact that study participants were mostly from training programs that generally have more male than female students. The ages of the respondents varied from 19 to 30 years and the average age was 22,5 years. The distribution of ages can be seen in the Figure 14.

[13] https://noppa.aalto.fi/noppa/kurssi/t-121.3110/etusivu

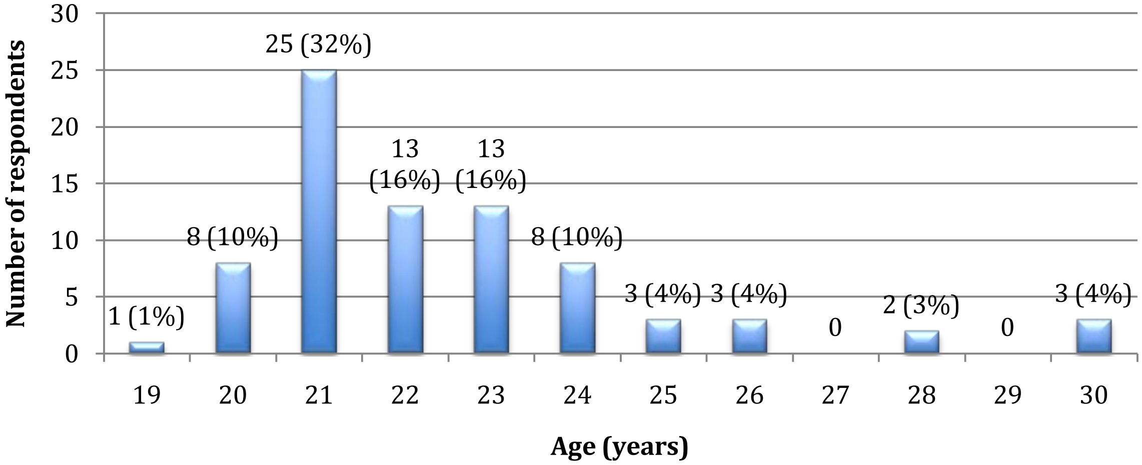


Figure 14. Age distribution of the respondents

The amount of respondents owning a smart phone was higher (48 of 79 respondents, 61%) compared to those who did not have one (31 of 79 respondents, 39%). A one-sample t-test between proportions was performed to determine whether there were significantly more of smart phone users than those not having one. The t-statistic was significant at the 0,05 critical alpha level, as t(78)=2,005 and the corresponding one-tailed probability p=0,0243.

The distribution between people who had installed applications to their phone (50 of 79 respondents, 63%) and those who had not installed (29 of 79 respondents, 37%) followed the same trend as smart phone ownership, and consequently there were significantly more of those who had installed application (t(78)=2,393, p=0,0096).

5 Results

This chapter presents the results of the empirical study. Firstly, the chapter explores the respondents' use habits. Secondly, the respondents' general attitudes and views are discussed. Thirdly, the chapter elaborates the respondents' awareness of the security mechanisms in mobile services and regular web services as well as the visibility of these mechanisms to users. Fourthly, the importance of perceived security in different use cases is discussed. Then, the chapter elaborates the factors that, according to the web survey, affect perceived security. Finally, the two last subchapters discuss the respondents' attitudes towards a mobile authentication solution that would utilize a security element in mobile phone as well as the suggestions that the respondents had for improving perceived security.

5.1 Use habits

In the beginning of the survey, general information about the respondents' use habits was collected. This information was considered to be necessary for the interpretation of the results, as it was assumed that all of the respondents would not have experience of mobile Internet and authentication. Another reason was that active users might differ from the average in their responses.

First, the usage of Internet services with mobile phone was enquired. The survey results show that a rather large proportion of the survey participants (31 of 79 respondents, 39%) use mobile Internet services daily. However, it was also noticed that almost a quarter of the respondents were never using mobile Internet despite their young average age and technical study background. A one-sample t-test between proportions was performed to determine whether there were significantly more of those who use mobile Internet than those who do not have experience of mobile Internet. The t-statistic was highly significant at the 0,01 critical alpha level, as t(78)=5,411 and the corresponding one-tailed probability p=0,0000. Figure 15 visualizes the use of mobile Internet in the whole group of respondents.

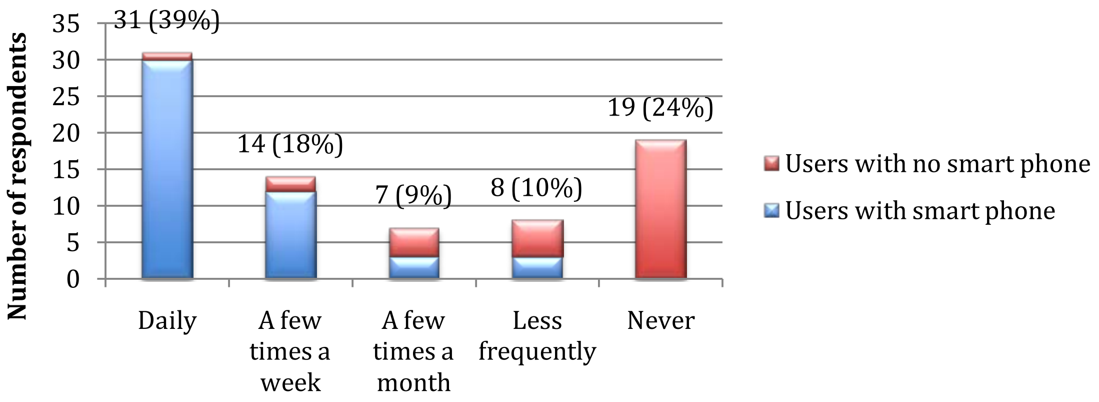


Figure 15. Use of mobile Internet among the respondents

The comparison between smart phone users and respondents who did not have a smart phone revealed that daily use of mobile Internet was considerably more popular among the smart phone users (30 of 48 respondents, 63%) than the other group of respondents (1 of 31 respondents, 3%). Consequently, majority of users that use mobile Internet daily or few times a week are smart phone users as can be seen from the Figure 15. It was also noticed that all of the survey participants that were never using mobile Internet were persons that did not have a smart phone. In the group of respondents not having a smart phone the proportion of people never using mobile Internet was as high as 61% (19 of 31 respondents).

Besides the mobile Internet usage, the participants were also asked how much they used mobile services that require authentication. The survey results show that fourth of the respondents (20 of 79 respondents, 25%) use these services daily and 19% (15 of 79 respondents) use the services a few times a week. This means that these two groups of people combined cover almost half of the survey respondents. However, the results also reveal that a considerable proportion of participants (27 of 79 respondents, 34%) never use authentication services with their mobile phones. Again, a one-sample t-test between proportions was performed to determine whether there were significantly more of those who use mobile services requiring authentication than those who did not have experience. The t-statistic was highly significant at the 0,01 critical alpha level, as t(78)=3,002 and the corresponding one-tailed probability p=0,0018. Figure 16 shows the breakdown of the participants’ use of mobile services requiring authentication.

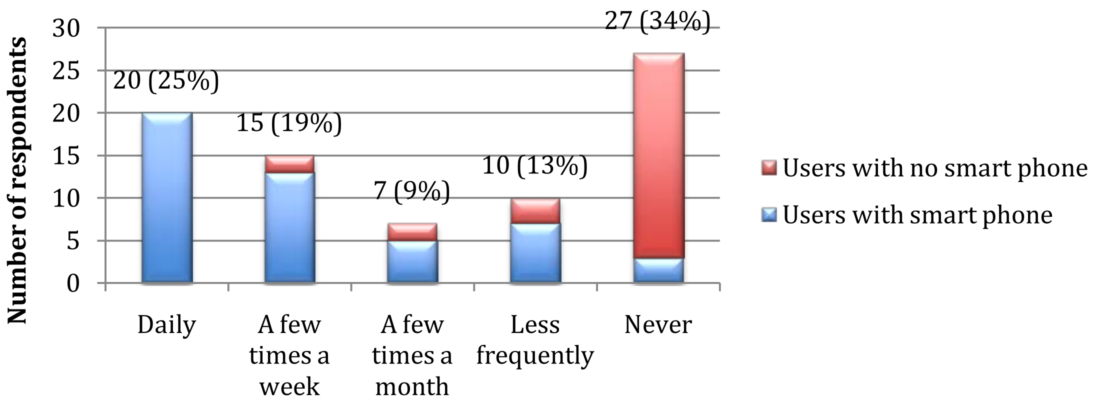


Figure 16. Use of mobile services requiring authentication among the respondents

When comparing the differences of the smart phone users and the users that did not have a smart phone, it turned out that 42% of the participants (20 of 48 respondents) owning a smart phone were using mobile authentication services daily and 27% of them (13 of 48 respondents) were using these services a few times a week. Only 6% of the smart phone users (3 of 48 respondents) were not using the services at all. By contrast, 77% of the respondents not having a smart phone (24 of 31 respondents) were never using mobile authentication services. The comparison reveals that the remarkable number of respondents that never use mobile authentication services largely originates from the group of respondents that do not have a smart phone (see Figure 16). When determining the relationship between usage of mobile Internet and usage of mobile services requiring authentication, it turned out that 61% of respondents that used mobile Internet daily were also using mobile services requiring authentication daily (19 of 31 respondents). Although majority of active mobile Internet users also actively used services requiring authentication, it needs to be noted that there is also a large number of active users that use mobile Internet mainly for activities that do not require authentication.

The respondents that did not use mobile services that require authentication were asked to answer the rest of the survey questions based on their experiences on authentication with a computer. Hence, a large proportion of the survey results will be presented as a comparison between mobile authentication users and computer authentication users. The group of respondents who had used mobile services involving authentication (n=52) will be referred to as **group A** or **mobile authentication users** for the rest of the thesis. On the other hand, the group that had no experience of mobile authentication, and thereby answered the questions from the perspective of authentication in regular Internet services used with a PC (Personal Computer) or laptop computer (n=27), will be referred to as **group B** or **computer authentication users** for the rest of the thesis. The differences in the answers between the group A (mobile authentication users) and group B (computer authentication users) are discussed when the comparison is considered to be meaningful.

5.2 General attitudes and views of users

This subchapter first presents the respondents' general attitudes regarding new mobile services or regular web services that are used with a PC or laptop. Secondly, the participants' general perceptions of authentication security as well as the changes in perception are explored. Lastly, the subchapter presents how much the respondents generally think of security while using services.

5.2.1 Attitude towards new (mobile) services

The web survey enquired the participants' general attitude towards new mobile services or regular web services. It turned out that in the case of both group A (mobile authentication users) and group B (computer authentication users), more than half of the respondents had a fairly trusting attitude towards new services. However, suspiciousness was clearly noticeable as a large proportion of the participants in both groups were fairly suspicious. The most extreme attitudes were quite rare as can be seen from Figure 17. It is, nonetheless, noteworthy that 8% of the respondents in the group A were very trusting, whereas none of the users in the group B were very trusting. It must also be noted that 11% of the users in the group B were very suspicious, while none of the respondents in the group A stated similarly.

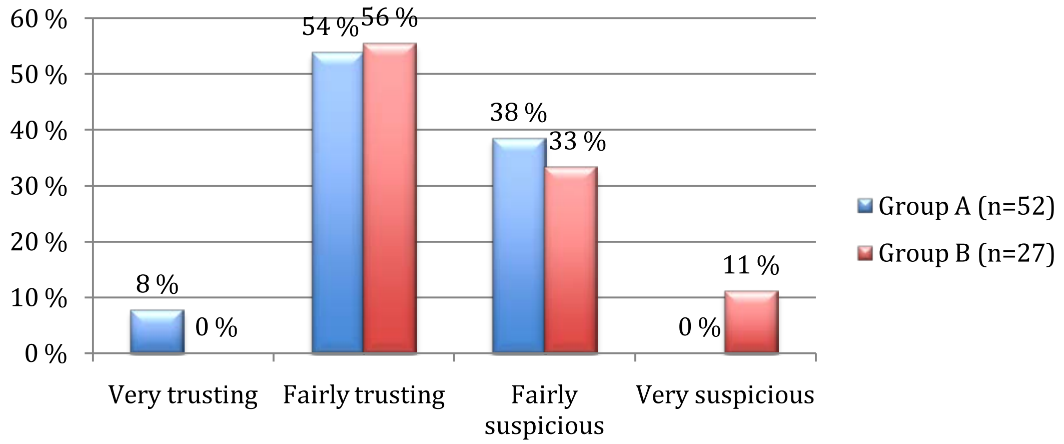


Figure 17. Respondents' general attitude towards new mobile services (or regular web services used with a PC or laptop)

For both the responses of group A and group B, a one-sample t-test between proportions was performed to determine whether there were significantly more of very trusting and fairly trusting participants than fairly suspicious and very suspicious participants. For the group A, the t-statistic was significant at the 0,05 critical alpha level, as t(51)=1,783 and the corresponding one-tailed probability p=0,0403. For the group B, on the other hand, the t-statistic was not significant at the 0,05 critical alpha level, as t(26)=0,628 and the corresponding one-tailed probability p=0,2677. Furthermore, a two-sample t-test between proportions was performed to determine whether there was a significant difference between groups A and B. The t-statistic was not significant at the 0,05 critical alpha level, as t(77)=0,516 and the corresponding two-tailed probability p=0,6072.

The most active mobile authentication users that use the services daily (referred to as **active mobile authentication users** for the rest of the thesis) had a little more trusting attitude towards new mobile services than the group A on average. 10% of mobile authentication users were very trusting and 55% of them were fairly trusting.

5.2.2 Perceived security of authentication

The survey participants were asked how they perceived the security while they authenticated to a mobile service or to a regular web service with a PC or laptop. The results show that the perceptions of the respondents were generally confident in both the group A and the group B. 71% of the mobile authentication users (group A) felt fairly secure, while the corresponding number in the group B was 85%. Some of the respondents in both groups even felt very secure. Despite the generally positive and confident perceptions, there were still respondents who felt that authentication was fairly insecure. In the group A, these participants made up almost fifth of the group. The respondents of the group B were less worried, as only 4% of them felt fairly insecure. None of the participants in either one of the groups felt completely insecure.

For both the responses of group A and group B, a one-sample t-test between proportions was performed to determine whether there were significantly more of those considering authentication as very secure or fairly secure than those considering authentication as very fairly insecure or insecure. For the group A, the t-statistic was highly significant at the 0,01 critical alpha level, as t(51)=5,698 and the corresponding one-tailed probability p=0,0000. For the group B, the t-statistic was also highly significant at the 0,01 critical alpha level, as t(26)=12,198 and the corresponding one-tailed probability p=0,0000. Furthermore, a two-sample t-test between proportions was performed to determine whether there was a significant difference between groups A and B. The t-statistic was not significant at the 0,05 critical alpha level, as t(77)=1,829 and the corresponding two-tailed probability p=0,0712. The respondents' security perceptions are illustrated in Figure 18.

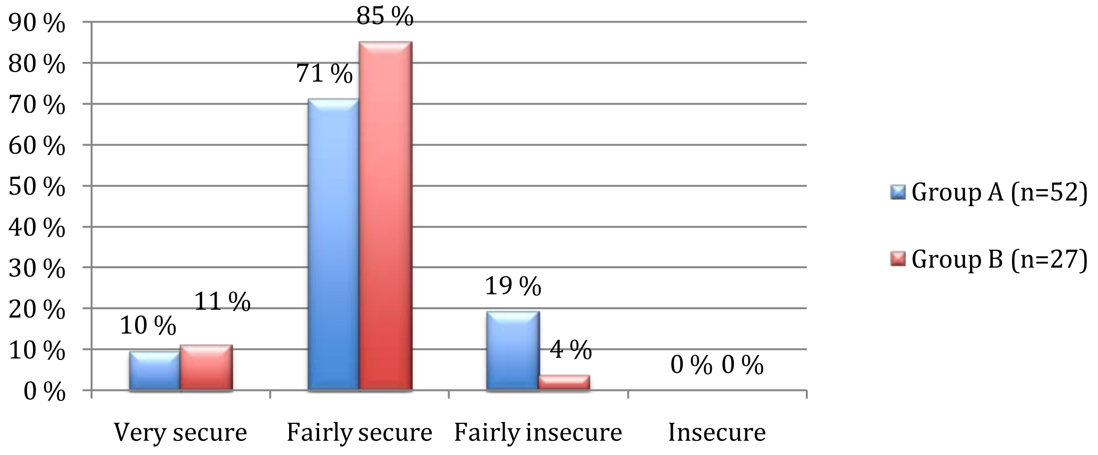


Figure 18. The respondents' general perceptions of mobile authentication security or security of authentication in standard web services

The active mobile authentication users differed somewhat from the average of the group A (mobile authentication users) when the distribution of the responses was examined. The amount of users that felt fairly secure is almost the same (70% versus 71%), but the active users felt quite significantly more secure than the average (20% versus 10%). Consequently, the amount of respondents feeling fairly insecure was also smaller in the group of active users (10% versus 19%).

To uncover changes in respondents' attitudes the web survey enquired whether the participants' general perceptions of the authentication security in mobile services or regular web services used with computer had changed. The majority of both the group A (62%) and the group B (63%) stated that their attitude had not changed. The rest of the respondents in both groups showed somewhat more change for the better than for the worse in their perceptions as can be seen from the Figure 19. The positive change in perceptions is greater among the mobile authentication users than computer authentication users. The active mobile authentication users did not differ considerably from the average in their attitudinal changes. This group of active users showed the least changes of all with 70% stating that their attitude had not changed.

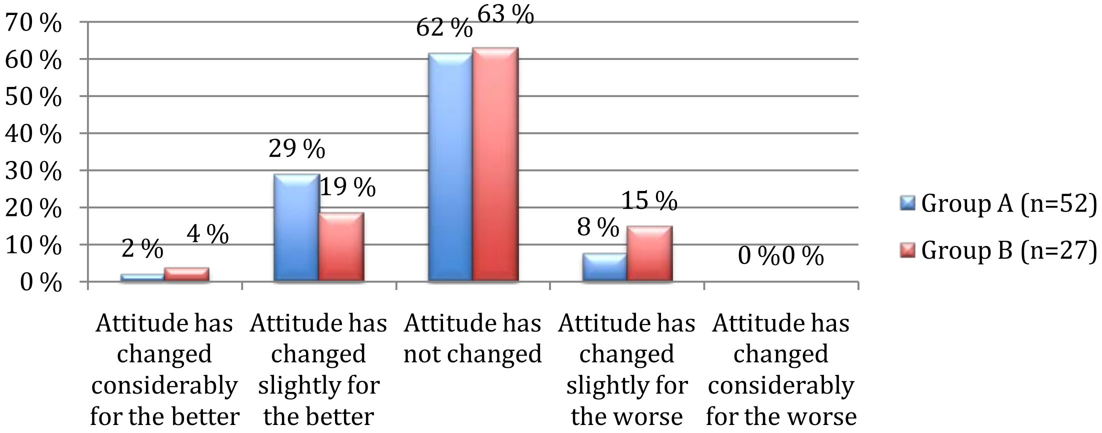


Figure 19. Changes in the respondents' attitudes towards perceived security of authentication in mobile services (or regular web services used with a PC or laptop)

5.2.3 The extent to which users think about security

The participants were also asked how much they generally thought about security when authenticating to mobile services or regular web services. Majority of both the group A (mobile authentication users) and the group B (computer authentication users) had either fairly much or fairly little of thoughts related to security. Smaller proportions of the respondents stated that they were thinking security much or little, and some of the respondents even said they were not thinking security at all. The results are shown in Figure 20. When comparing the group A and B, it can be seen that the respondents in group B were thinking about security generally a little more than the respondents in group A, although the difference is not substantial. The active mobile authentication users did not differ considerably from the average of group A.

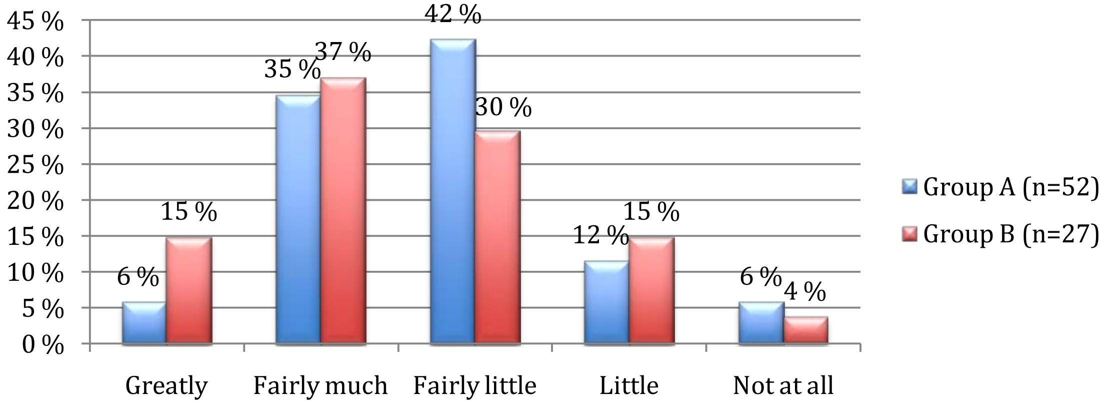


Figure 20. The extent to which the respondents think of security when authenticating in the services

5.3 Security mechanisms

This subchapter first explores the participants' awareness of the security mechanisms utilized in the services. Then the subchapter presents information of how visible the respondents consider the security mechanisms to be while using services.

5.3.1 Respondents' awareness of security mechanisms

The general security knowledge of the study participants was also considered as an important aspect so this was enquired in the web survey. The respondents were asked about their awareness of the security features or mechanisms that are utilized in mobile services or in regular web services that are used with computer. It turned out that mobile authentication users considered themselves as relatively unaware of the security features as 44% of the respondents in the group A (23 of 52 respondents) stated that they were fairly little aware of the features and 21% (11 of 52 respondents) responded that they were only little aware. Thus, these two groups of respondents alone cover over 60% of all responses in the group A. However, 25% of the mobile authentication users (13 of 52 respondents) considered themselves as either well aware or fairly aware of the security features (10 of 52 respondents). The respondents in the group B (computer authentication users) were overall more aware of the security features than the respondents in the group A. The amount of either well aware (2 of 27 respondents) or fairly aware respondents (10 of 27 respondents) in the group B was 44%, which is considerably more than in the group A. However, more than half of the respondents in the group B still showed relatively modest awareness of the security features.

For both the responses of group A and group B, a one-sample t-test between proportions was performed to determine whether there were significantly more of those respondents being fairly little aware, little aware or unaware of the security features than those being well aware or fairly aware. For the group A, the t-statistic was highly significant at the 0,01 critical alpha level, as t(51)=4,163 and the corresponding one-tailed probability p=0,0001. For the group B, on the other hand, the t-statistic was not significant at the 0,05 critical alpha level, as t(26)=0,628 and the corresponding one-tailed probability p=0,2677. Furthermore, a two-sample t-test between proportions was performed to determine whether there was a significant difference between groups A and B. The t-statistic was not significant at the 0,05 critical alpha level, as t(77)=1,724 and the corresponding two-tailed probability p=0,0886. The awareness of respondents is visualized in Figure 21.

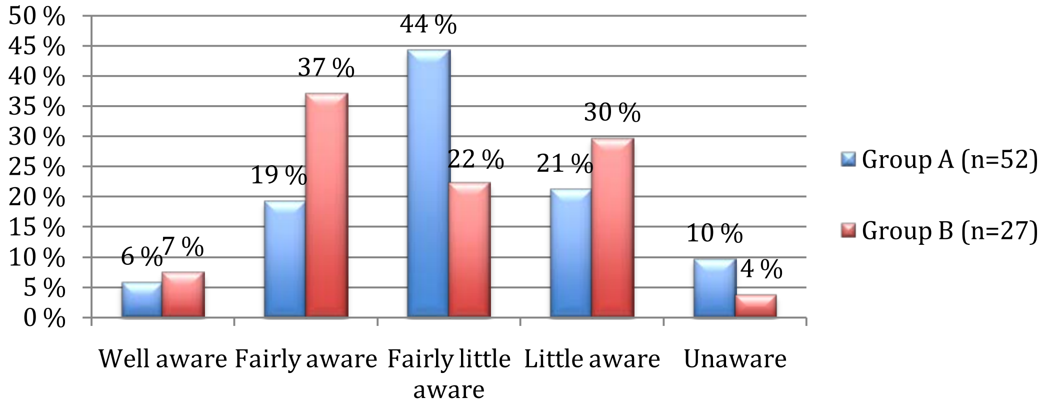


Figure 21. Respondents' awareness of the security features/mechanisms utilized in mobile services (or regular web services used with computer)

The active mobile authentication users did not differ considerably in their security awareness from the average of the group A. They turned out to be a little more aware on average, but on the other hand, the amount of completely unaware respondents in this group of active users was a little higher than average.

5.3.2 Visibility of security mechanisms

The survey enquired the visibility of security mechanisms to users with an open-ended question. The responses show that a large proportion of the respondents did not observe underlying security mechanisms very much (15 statements) or at all (12 statements). When looking at how these statements were divided between the group A and the group B, it appears that approximately fifth of the respondents in both groups stated that they do not perceive security features very much. The proportion of respondents who did not perceive security mechanisms at all is, however, somewhat larger among the mobile authentication users (17% in group A and 11% in group B).

The respondents that had observed security mechanisms in services that require authentication expressed a few different ways of how security is visible to them. Almost half of the respondents stated that they were aware of the signs that show the connection is encrypted (38 statements). In their responses, respondents mostly mentioned the lock sign in the Internet browser indicating SSL encryption as well as the https prefix in the URL. In their statements of how security is visible the respondents also mentioned password inquiry (19 statements), information dialogs of secured or unsecured connection (10 statements) and certificates (11 statements). When comparing the responses of the group A and B, it turns out that the statements of secured connection are more common among the computer authentication users (56% of the group B commenting) than among the mobile authentication users (44% of the group A commenting), indicating less visible information of encrypted connection in mobile services. The difference in password inquiry statements was smaller, as 26% of the group B gave these statements compared to 23% in the group A. The comparison of information dialog statements revealed a larger difference with 4% in the group B and 17% in the group A. In certificate statements the difference was marginal, as the percentages were 15% in the group B and 13% in the group A.

5.4 Factors that affect perceived security

This subchapter presents the factors that, according to the results of the empirical study, affect the respondents' perceived security in mobile services and regular web services.

5.4.1 User's observation of security mechanisms

As the web survey examined respondents' awareness of security features and mechanisms, it was also logical to figure out how much the observed security mechanisms affected the security perceptions of the respondents. It turned out that majority of the respondents felt that seeing indications of security was important for the perceived security. Over 60% of the respondents both in the group of mobile authentication users (group A) and the group of computer authentication users (group B) expressed that perceived security features affected their perception of security either greatly or fairly much (see Figure 22). However, the proportions of the respondents that did not consider signs of security so important were also relatively large. The active mobile authentication users did not differ significantly from the average of group A.

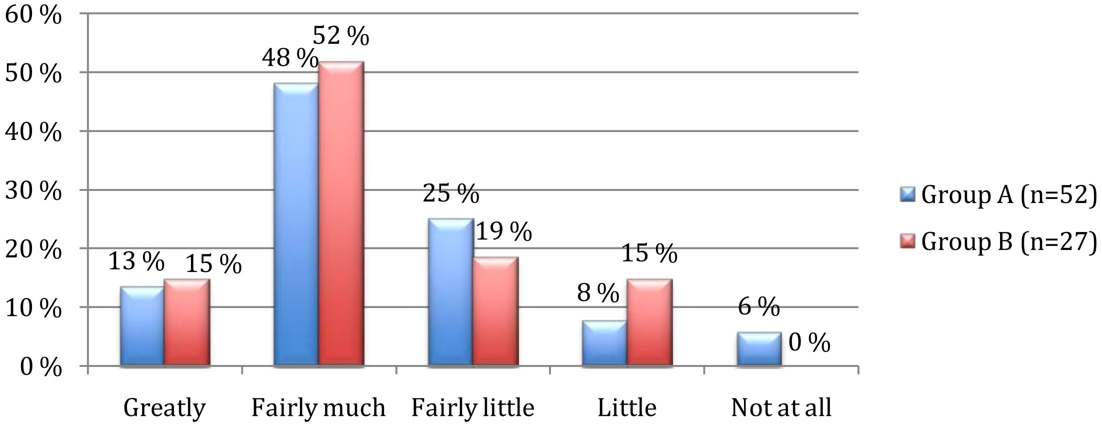


Figure 22. The extent to which respondents felt observed security features affected their perception of security

For both the responses of group A and group B, a one-sample t-test between proportions was performed to determine whether there were significantly more those considering observed security features as affecting perceived security greatly or fairly much than those considering observed security features as affecting fairly little, little or not at all. For the group A, the t-statistic was not significant at the 0,05 critical alpha level, as t(51)=1,626 and the corresponding one-tailed probability p=0,0551. For the group B, on the other hand, the t-statistic was significant at the 0,05 critical alpha level, as t(26)=1,879 and the corresponding one-tailed probability p=0,0358. Furthermore, a two-sample t-test between proportions was performed to determine whether there was a significant difference between groups A and B. The t-statistic was not significant at the 0,05 critical alpha level, as t(77)=0,524 and the corresponding two-tailed probability p=0,6017.

5.4.2 Device

The survey explored also how the device with which the authentication takes place affects perceived security. The respondents were asked which alternative they considered as more secure: authenticating with computer or with mobile phone. As can be seen from the Figure 23, the results were quite different for mobile authentication users (group A) and computer authentication users (group B). The majority of the respondents in group A (65%) thought that computer is more secure device for authentication, while only 33% of the respondents in group B responded similarly. Mobile phone was not favored by either of the groups as more secure, as none of the mobile authentication users were voting for it, and only 7% of the group B considered mobile phone as more secure device for authentication. The amount of respondents that did not see difference between the two devices was high (59%) in the group B, whereas only 35% of the respondents in group A thought similarly. In the group A, the active mobile authentication users did not differ from the average.

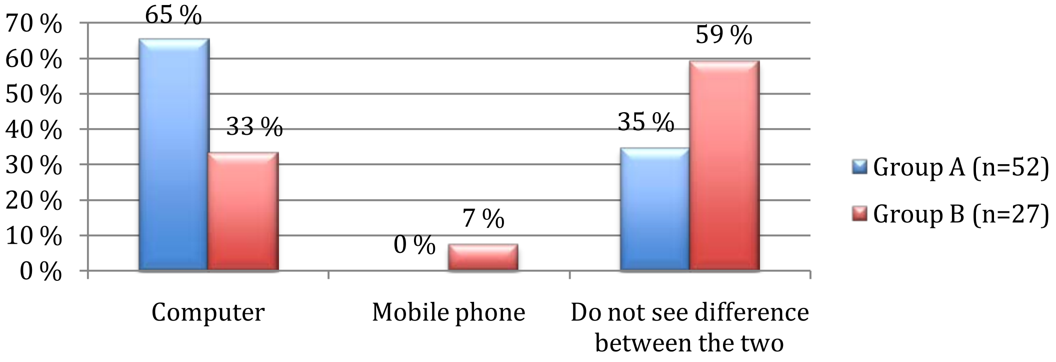


Figure 23. Respondents' opinions of which device was perceived more secure for authentication

For both the responses of group A and group B, a one-sample t-test between proportions was performed to determine whether there were significantly more those considering computer as more secure than those considering mobile phone as more secure. For the group A, the t-statistic was highly significant at the 0,01 critical alpha level, as t(51)=9,827 and the corresponding one-tailed probability p=0,0000. For the group B, the t-statistic was significant at the 0,05 critical alpha level, as t(26)=2,343 and the corresponding one-tailed probability p=0,0270. Furthermore, a two-sample t-test between proportions was performed to determine whether there was a significant difference between groups A and B. The t-statistic was significant at the 0,01 critical alpha level, as t(77)=2,707 and the corresponding two-tailed probability p=0,0084.

The respondents' statements from the open-ended questions highlight several reasons why mobile phone is perceived less secure device for authentication than PC. One of these reasons was the concern that mobile phone would freeze during the authentication. Some respondents also commented their anxiety regarding breakdowns in mobile Internet connection as well as the slower Internet browsing capabilities of mobile phones compared to computers. A few respondents had experienced requests to log in again during the use of mobile services, which increased their suspicion. One reason for security concerns and increased doubts was also the fact that the many respondents have only little experience of mobile service use and mobile Internet is relatively new for them. Many respondents also expressed thoughts regarding virus protection and firewall, and stated that they were unaware of how the lack of these elements in mobile phones affected the security. The responses revealed that many respondents considered traditional computing environment safer because of virus protection and firewall. The comments of the respondents also revealed that a major reason for considering mobile environment less safe than traditional computing environment is that users are accustomed to computer use, which increases their confidence and perceived security. Only a few of the respondents stated that mobile services involve less security threats than regular computer services because computers are still the main targets of hackers. Additionally, a couple of respondents highlighted the fact that there has been very few, if any reported misuse cases in mobile environment. All in all, many of the survey responses reveal that users have little information of security in mobile environment compared to traditional computing environment, and therefore most people form their conceptions of mobile security based on mental impressions rather than knowledge.

The physical characteristics of mobile phones got also attention in some of the survey responses. Small screen size as well as slowness and inconvenience of writing with a mobile phone were commented particularly. Limited screen area was stated to make it difficult for the user to see all of the important information at a glance, and poor writing capabilities were claimed to both make writing slow and increase the likelihood of typing errors. These aspects were considered to increase uncertainty of mobile service use and therefore also affect perceived security. Many respondents considered computer as a more convenient device to use and therefore they felt more confident using it for certain services instead of mobile phone.

Many respondents also clearly expressed that they are generally more careful about mobile services than services they use with a computer. A great number of respondents did not comment on whether the differences between the device types affected their intention to use mobile services, although this was directly enquired in the survey.

5.4.3 Type of service

The respondents' opinions on the criticality of security in different service types were explored in an open-ended survey question. The results show that almost all of the respondents (74 out of 79, 94%) thought that security is especially important when money is involved in the use of the service. Both the group of mobile authentication users and computer authentication users share this view. Many of the mobile authentication users (23 of 52 respondents in group A, 44%) stated that they do not use banking services with mobile phone due to skepticism towards mobile data security and also the perceived inconvenience compared to traditional computing environment. A few respondents in the group A (6 of 52 respondents, 12%) also expressed their unwillingness to make large purchases with mobile phone. Despite the concerns of many respondents, still slightly over half of the group A expressed that there are no mobile services they would not use due to security concerns (27 statements). However, some of these respondents stated that they still prefer computer to mobile phone if they have the possibility to choose between the two.

A large proportion of the respondents (33 of 79, 42%) considered security as crucial also in authentication procedures where personal data is transferred. There were more of these statements among the computer authentication users (63%) than the mobile authentication users (31%). The respondents mentioned also social media services in their statements regarding where security matters the most. 17 respondents highlighted the importance of security in social media services in their responses and the statements also clearly showed the respondents' suspicion towards the security of Facebook. When comparing the group A to group B, it shows that the importance of social media security is less emphasized among the mobile authentication users (17%) than the computer authentication users (30%). Although many respondents highlighted the importance of security, there were also almost as many respondents stating that security is not so crucial in social media services (15 statements). Potential harm of misuse was not considered to be very critical according to the statements of many of these respondents. All of the statements except for one were found from the group of mobile authentication users. Similarly to social media services, also the importance of security in email was perceived inconsistently among the respondents. 14 respondents considered security to be particularly important in email services. The importance of email security was highlighted less among the mobile authentication users (13%) than the computer authentication users (26%). By contrast, 14 respondents were not worried of security in email services. All of these respondents were from the group of mobile authentication users.

The survey responses show that almost half of the respondents thought that security is less important in services of entertainment purposes such as gaming, news services and web forums (37 respondents). Many of these respondents stated, for example, that if someone unauthorized got access to their account, it would not enable the intruder to do much harm, as the account in these kinds of services often only allows the user to see more information or access more features. Many respondents also thought that it is unlikely that someone would be interested to seek access to this kind of personal account. Although a great number of respondents were able to point out services where security is crucial and services where it has less importance, there were also some respondents who stated that security is always important regardless of the service (7 statements).

5.4.4 Use context

The survey explored the respondents' opinions of the effect of use context to perceived security with an open-ended question. 59% of the participants (47 of 79 respondents) stated that the use context and environment affects their perception of security. 33 of these respondents were from the group A, meaning that 63% of mobile authentication users saw use context as a determining factor for perceived security. On the other hand, 14 of the respondents from the group B (52%) considered use context as a factor affecting perceived security. The results clearly show that use context affects the security perceptions of the respondents whether they have experience of mobile authentication or not. Nevertheless, the effect is somewhat greater in the case of mobile services. A minority of 29% (23 of the 79 respondents) stated that use context does not affect their perception of authentication security. 15 of these 23 respondents were from group A meaning that 29% of mobile authentication users did not see use context as an important factor affecting perceived security. 8 of the 23 respondents were from group B meaning that 30% of computer authentication users did not see use context as an important factor affecting perceived security.

For both the responses of group A and group B, a one-sample t-test between proportions was performed to determine whether there were significantly more of those considering use context as affecting perceived security than those considering use context not having effect on perceived security. For the group A, the t-statistic was highly significant at the 0,01 critical alpha level, as t(51)=2,734 and the corresponding one-tailed probability p=0,0043. For the group B, on the other hand, the t-statistic was not significant at the 0,05 critical alpha level, as t(26)=1,301 and the corresponding one-tailed probability p=0,1023. Furthermore, a two-sample t-test between proportions was performed to determine whether there was a significant difference between groups A and B. The t-statistic was not significant at the 0,05 critical alpha level, as t(77)=0,944 and the corresponding two-tailed probability p=0,3483.

Looking at the respondents' explanations for their responses reveals that the most remarkable concern of the respondents is that somebody would spy on them and see their password when authenticating in public places such as busses, shopping malls and cafes. Part of the respondents specified their responses by stating that they were worried of someone stealing their phone after finding out the password or when the user has entered username and password and is logged into the service. All in all, statements related to loss of mobile phone were rather common among the respondents as 22 respondents expressed their fear of losing mobile phone in the case of theft or other incident. In the case of many respondents, this concern had a negative effect on the intention to use especially banking services with mobile phone in certain places.

There was also a group of respondents that did not feel comfortable with authenticating in open wireless networks because of the potential threat of hacking (12 statements). Not only mobile authentication users but also computer authentication users who use their laptop computers in wireless networks expressed this concern in the survey responses. Many of these respondents stated that they do not use especially banking services in open wireless networks due to security risks. Some of the respondents in the group A stated that they do not pay for mobile Internet so they only use Internet in wireless networks, and the security of open networks limits the use of certain services. Part of the respondents in the group A using Internet in mobile network mentioned that they were worried of mobile data transfer security (10 statements). The responses reveal that unawareness of security level in mobile network is the primary reason for the suspicion. Only one respondent stated that authentication in mobile 3G network is well secured and that he prefers 3G connection to wireless even when using Internet with a laptop computer. In addition to respondents who specified their concerns to open wireless networks or mobile network, there were also some respondents who stated that they perceived wireless connection overall as insecure (9 statements).

All of the respondents that commented on the place where they felt the most secure when authenticating mentioned home in their responses. Additionally, some of these respondents expressed that also other home-like places such as a friend’s apartment were considered as safe environments.

5.4.5 Authentication provider

The survey participants were asked whether it affected their security perceptions that the authentication was provided by a third party company or by the service provider itself. The responses were distributed rather evenly as almost half of the participants in both the group of mobile authentication users (46%) and the group of computer authentication users (48%) felt that the provider of authentication affected perceived security, whereas a little more than half of the respondents did not see any difference. Looking at the responses of open-ended survey questions reveals that the respondents generally expressed more preference for authentication provided by a well-known third-party authentication provider (11 statements) than for authentication provided by the service provider itself (3 statements). Authentication through Internet banking service was most commonly mentioned as the preferred means of third-party authentication.

The respondents' opinions regarding third-party actors in authentication was also further explored by asking whether the perceived security of the authentication provided by a third-party actor is considered the same regardless of the service in which it is utilized. Majority (67%) of the respondents in both of the groups A and B perceived the security of a third-party authentication similarly in all services. Nevertheless, there were a rather significant 33% of the respondents in both groups, who perceived the security of third-party authentication differently depending on the service where the authentication takes place. For both the responses of group A and group B, a one-sample t-test between proportions was performed to determine whether there were significantly more those perceiving security of third-party authentication similarly regardless of the service than those stating that there is a difference. For the group A, the t-statistic was highly significant at the 0,01 critical alpha level, as t(51)=2,607 and the corresponding one-tailed probability p=0,0060. For the group B, the t-statistic was significant at the 0,05 critical alpha level, as t(26)=1,879 and the corresponding one-tailed probability p=0,0358.

5.4.6 Brand and reputation

As the effect of brands to perceived security was highlighted in many studies, it was also examined in the study of this thesis. In the web survey we asked how much effect did the respondents perceive the brand and the reputation of the authentication provider to have on their perception of security. Based on the results it is clear that brands affect perceived security considerably. A great majority of the survey participants in both the group A (85%) and the group B (85%) felt that brands affected the security perceptions either greatly or fairly much. Only a minor share of the respondents did not see brands as a factor affecting perceived security. The results are illustrated in Figure 24. The differences between mobile authentication users and computer authentication users were quite small.

The only noteworthy difference is that only the group A had users who thought the brands did not affect perceived security at all or only affected a little.

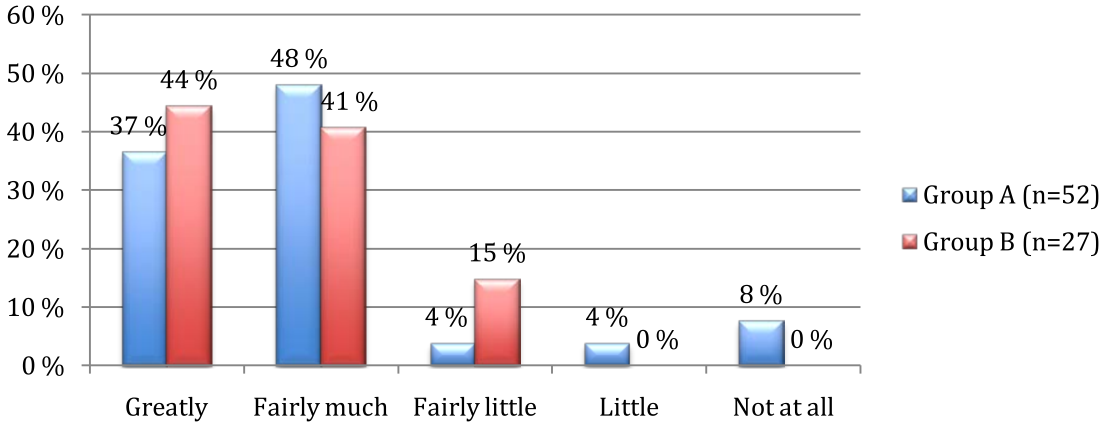


Figure 24. The effect of brand name and reputation on the respondents' perceived security

For both the responses of group A and group B, a one-sample t-test between proportions was performed to determine whether there were significantly more of those considering brand name and reputation as affecting perceived security greatly or fairly much than those considering brand name and reputation as affecting fairly little, little or not at all. For the group A, the t-statistic was highly significant at the 0,01 critical alpha level, as t(51)=7,068 and the corresponding one-tailed probability p=0,0000. For the group B, the t-statistic was also highly significant at the 0,01 critical alpha level, as t(26)=5,093 and the corresponding one-tailed probability p=0,0000.

The survey explored the respondents' opinions on which companies they perceived as trustworthy authentication providers. Banks were most commonly mentioned in the responses as 40 out of 79 respondents (51%) expressed their trust for banks. The most common reasoning (13 statements) was that banks utilize lists of variable passwords in authentication, which the respondents perceived as secure. In addition, 6 other respondents expressed their preference for variable passwords in the other questions of the web survey. This means that approximately fourth of the survey respondents valued the use of variable passwords. Another common explanation (8 statements) for perceiving banks as trustworthy actors was that banks cannot afford making serious mistakes because this might lead to loss of reputation and that taking care of security is also the advantage of the banks. A few respondents (3 statements) stated that they had confidence in banks because they have long-term experience of keeping the customers' money safe.

The survey responses also clearly show that many of the respondents consider well-known and widely recognized authentication providers (45 statements) as well as large companies (19 statements) as trustworthy. Examples include actors such as public administration, universities, Haka federation and Luottokunta. Many respondents also especially accentuated Finnish service providers as the ones they trusted the most. A few respondents also highlighted well-known, foreign companies such as PayPal and Google as trustworthy service providers. Some respondents, however, openly expressed their suspicion for foreign actors.

5.4.7 Amount of service usage experience

The respondents were asked if the amount of experience they had from the service usage affected perceived security. More than half of the respondents (44 out of 79, 56%) stated that the amount of experience has effect on perceived security. Majority of the respondents did not specify their responses by explaining how the experience affected, but those who did, most commonly stated that experience helps in recognizing the security risks (17 statements). A few respondents expressed that as the amount of service usage experience increases, they get accustomed to the use and feel more comfortable, which also improves the feeling of security. Some users also expressed that having used a certain service with a computer makes them feel more comfortable using it with a mobile phone, too. Although over half of the respondents thought that the amount of experience affects perceived security, there were still 22 respondents (28%) who thought that the amount of experience does not have effect on perceived security. Part of the respondents did not answer the question or stated that they did not have a clear opinion on the question.

A one-sample t-test between proportions was performed to determine whether there were significantly more of those considering amount of service usage experience as affecting perceived security than those thinking that usage experience does not have effect on perceived security. The t-statistic was highly significant at the 0,01 critical alpha level, as t(78)=2,852 and the corresponding one-tailed probability p=0,0028.

5.4.8 Own positive and negative experiences

The significance of past positive and negative experiences was explored in the web survey by asking the participants how much they felt that past good or bad experiences of either mobile services or regular web services affect perceived security when starting to use a new service. As can be seen from Figure 25, 50% of mobile authentication users and 59% of computer authentication users thought that experiences affect perceived security either greatly or fairly much, which clearly shows that experiences are an important factor in determining perceived security. The groups A and B differ most strongly in the amounts of respondents who thought that the experiences affect perceived security fairly little or little. The high percentage of mobile authentication users stating that experiences have a fairly little effect on perceived security is most probably due to the fact that many of the respondents giving these responses had possibly not used mobile services for a long time and therefore did not have many previous experiences that could have affected perceived security. The effect of own experiences on perceived security was considered a little more important among the active mobile authentication users than the average of group A.

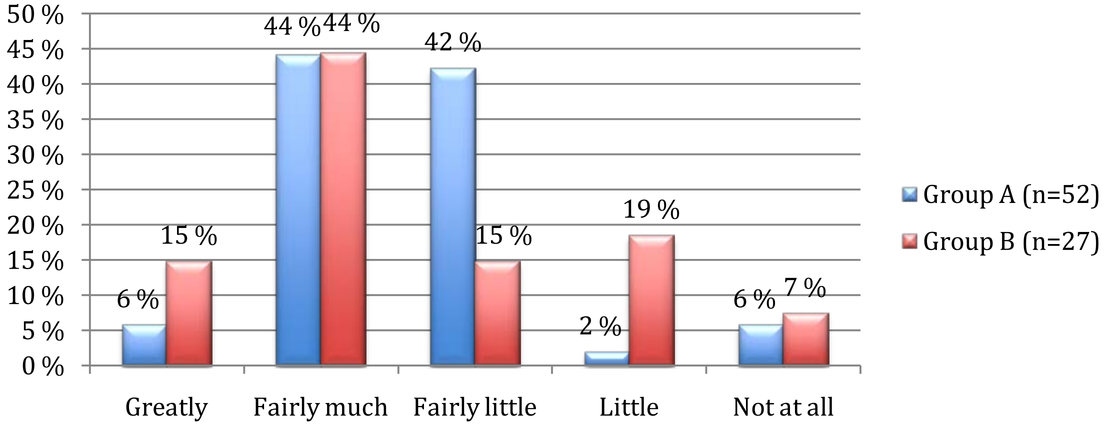


Figure 25. The extent to which survey participants felt past experiences affect perceived security when taking a new service into use

For both the responses of group B, a one-sample t-test between proportions was performed to determine whether there were significantly more those considering own positive/negative experiences as affecting perceived security greatly or fairly much than those considering own experiences as affecting fairly little, little or not at all. For the group A, the test was not performed since the distribution was 50%/50%. For the group B, the t-statistic was not significant at the 0,05 critical alpha level, as t(26)=0,951 and the corresponding one-tailed probability p=0,1752. A two-sample t-test between proportions was performed to determine whether there was a significant difference between groups A and B. The t-statistic was not significant at the 0,05 critical alpha level, as t(77)=0,760 and the corresponding two-tailed probability p=0,4494.

The effects of positive and negative experiences on perceived security were explored further with an open-ended survey question. 47% of the study participants (37 of 79 respondents) expressed that negative experiences of a certain service will increase their suspiciousness for the services in general. On the other hand, 43% of the study participants (34 of 79 respondents) stated that positive experiences increase their confidence in the security of the services. In many of the survey responses, only the effect of negative experiences was commented, indicating a stronger effect of bad experiences compared to good ones. Some of the respondents even directly stated that positive experiences do not have as great effect on perceived security as negative experiences, since good experiences are expected to be a default. 18% of the study participants (14 of 79 respondents) commented that they do not let the experiences from one service greatly affect the attitude towards other services. However, many of these respondents stated that the experiences could affect the attitude towards services that are provided by the same company as the service from which they have experiences. Furthermore, experiences can have effect if the service much resembles certain service the user has experiences of, although the service provider would be different.

5.4.9 Experiences and recommendations of others

In addition to the participants' own experiences, they were also asked how much they felt that experiences and recommendations of acquaintances and friends affected perceived security of authentication. As Figure 26 shows, the majority of the respondents in both the group A (65%) and the group B (59%) considered friends' opinions to have either great influence or fairly much influence on security perceptions. In the light of these results it can be stated that experiences and recommendations of acquaintances and friends are one important factor that affects perceived security of authentication both in mobile services and regular web services. The active mobile authentication users regarded others' experiences and recommendations as having a little less effect on perceived security than the average of group A, and 10% thought they had no effect.

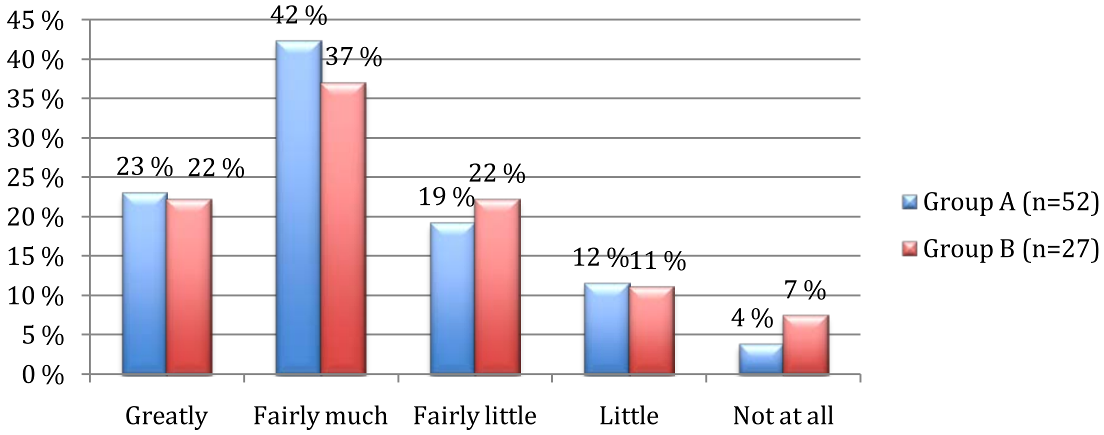


Figure 26. The extent to which survey participants felt experiences and recommendations of acquaintances and friends affecting perceived security of authentication in mobile services or standard web services

For both the responses of group A and group B, a one-sample t-test between proportions was performed to determine whether there were significantly more those considering experiences and recommendations of others as affecting perceived security greatly or fairly much than those considering others' experiences as affecting perceived security fairly little, little or not at all. For the group A, the t-statistic was significant at the 0,05 critical alpha level, as t(51)=2,268 and the corresponding one-tailed probability p=0,0138. For the group B, on the other hand, the t-statistic was not significant at the 0,05 critical alpha level, as t(26)=0,951 and the corresponding one-tailed probability p=0,1752. Furthermore, a two-sample t-test between proportions was performed to determine whether there was a significant difference between groups A and B. The t-statistic was not significant at the 0,05 critical alpha level, as t(77)=0,524 and the corresponding two-tailed probability p=0,6020.

The effect of others' experiences was not further explored with an open-ended question, but some of the respondents mentioned the topic in some of the other questions. These comments revealed that besides hearing experiences of friends and acquaintances, users also search for other people's experiences from certain Internet forums, for example.

5.4.10 Look and feel

Examining the responses of open-ended survey questions reveals certain aspects of look and feel that either improve or decrease perceived security of a service that involves authentication. The visual characteristic that was often mentioned as being a factor improving perceived security was clearness (24 statements). Many of these responses indicated that users only want to see necessary elements and information in a neatly organized layout. 12 respondents also directly stated that they preferred simplicity (fin. “yksinkertaisuus”) in the visual appearance. Several respondents highlighted that professional appearance (fin. “ammattimainen ulkoasu”, 16 statements), correctness (fin. “asiallisuus”, 15 statements) and formality (fin. “virallisuus”, 7 statements) improves security perceptions and trust. A great number of respondents also expressed that visually pleasant, well-groomed (fin. “huoliteltu”) appearance is important for feeling of security (24 statements). Many of the respondents commented that this makes the user think that the company takes good care of things, including security. Also modernity of the appearance was perceived as an indication of up-to-date security procedures. Furthermore, some respondents thought that use of quiet colors such as certain shades of blue in the graphical user interface of a service affects perceived security positively (9 statements). Another visual aspect improving perceived security that a few respondents mentioned was placement of the logo of a trustworthy company visibly in the service. Regarding the textual content of the graphical user interface, some of the respondents highlighted that showing the essential information about security implementation of the service clearly to the user has a positive effect on perceived security (7 statements). Some respondents also mentioned that making the contact information of the service provider easily available for the user increases trust (5 statements). Having a physical place of business and showing proof of it was also highlighted in a few responses. Many respondents expressed that openness towards the service user effectively dispels suspicions regarding the trustworthiness of a company.

On the negative side, many respondents articulated that ambiguous (fin. “epäselvä”) and disorganized (fin. “sekava”) appearance decreases perceived security of a service (17 statements). Besides the fact that this kind of a graphical user interfaces are difficult to understand and use, they were also stated to give users a feeling that the service provider is trying to hide something behind the disordered façade. Examining the responses also revealed that several respondents considered amateurish appearance as a factor affecting security perceptions negatively (16 statements), as this might, for example, indicate incompetence of the service provider to implement a secure service. Furthermore, many respondents highlighted that their perception of security decreases if a service looks clumsy (fin. “tökerö”) and appears to be implemented very quickly and negligently (14 statements). Several respondents reported that this kind of appearance gives an impression that also security is implemented carelessly in the service. For many of the respondents, a major factor decreasing perceived security was advertisements (21 statements). Some of these respondents were not expecting a service completely free of advertisements, but stated that excessive advertisements affected negatively. There were also a couple of respondents who considered a complete lack of advertisements potentially suspicious. Besides the advertisements, many respondents mentioned that also other distracting content such as flash videos and unnecessary images decreased perceived security (15 statements). Moreover, a few respondents noted that poor quality of images and other graphics in the service affect perceived security negatively. The use of colors was also commented in context of aspects that weaken perceived security, as several respondents mentioned the negative effect of strange color choices, use of glaring colors and excessive color use (18 statements). Another negatively affecting visual aspects that received some attention in the survey responses were unpleasant appearance, unfamiliar logos and unusual fonts. Many respondents also highlighted the importance of the textual content of a service for perceived security, and stated that careless and flawed text and content, mixed use of languages, and use of odd and unfamiliar terminology are examples of aspects that have a negative effect on perception of security (12 statements).

Besides the visual aspects, the respondents also commented other aspects related to the usage and functionalities of services. In order to feel secure, many respondents stated that the graphical user interface has to be fluent and workable (9 statements). Some respondents also mentioned reliability and stability of the service as important aspects, and stated that the service is, for example, not allowed to seize up during authentication. A few respondents highlighted mobile-optimized user interfaces in their statements about aspects that positively affect security perception. Use of common conventions in the user interface design was also often mentioned to have positive effect on perceived security, as it was stated to facilitate navigation and give a feeling of familiarity (7 statements). Uncommon design solutions, inconsistencies and obvious design flaws, on the other hand, were stated to have negative effect. The respondents commonly noted that information about the consequences of performed actions as well as practices in handling the confidential data generally improves perceived security (7 statements). Availability of clear use instructions (3 statements), troubleshooting information (3 statements) and comprehensible terms of use (3 statements) were also mentioned in the survey responses. Some respondents directly expressed that ease-of-use or usability improved their feeling of security (4 statements). On the other hand, there were many respondents stating that the authentication procedure should be complex enough so that it feels secure (9 statements). However, it was commonly noted by the respondents that too much complexity leads to frustration and feeling of bad usability, so finding a balance between complexity and usability was considered to be essential. Overall, the respondents did not clearly specify what they meant with enough complexity. A few of the respondents who elaborated their thoughts mentioned authentication with online banking passwords, confirmations for all critical actions and mandatory authentication each time when using the service (i.e. no for automatic authentication and remembering passwords).

The vast majority of the survey respondents clearly expressed that they pay attention to the look and feel of the service, and that it strongly affects the way security is perceived. Only a small proportion of the respondents stated that the visual appearance of the service does not have much effect or any effect at all (12 statements). When the survey responses regarding the look and feel of a service are examined carefully, it can be noticed that the respondents generally commented negative aspects more emphatically and often before the positive aspects. Many of the responses imply that negative factors have more effect on the formation of perceived security than positive ones. Some respondents even directly stated that positive characteristics are considered as a standard rather than something extraordinary that improves perceived security considerably.

5.5 Mobile authentication with a built-in security element

As this thesis was done within the MoFS (Mobile Financial Services) project that has interests for developing new ways to enable secure mobile authentication, the survey included two questions enquiring the respondents' opinions of authentication that utilizes a security element that is built inside a mobile phone. The operating principle of security element was not explained in detail, but the aim was to gather general opinions and attitudes about this sort of mechanism that would enable authentication to certain services. 19 of the 79 respondents (24%) expressed positive opinions regarding the authentication utilizing the security element and stated that they would use it in all services for which it would be available as an authentication mechanism. 31 of the 79 respondents (39%), in turn, were more careful with their statements and expressed that they would use the security element for authentication with certain conditions or only in certain types of services. 17 of the 31 (55%) respondents stated that they would only use the security element in services that do not involve too much sensitive, personal information. Thus, majority of these respondents expressed their unwillingness to use the security element in banking services or other services involving money. Some of the respondents, in turn, stated that they would use the security element for authentication provided that it is proved to be absolutely secure (6 statements), or if it would paired with password (5 statements). Although having a positive attitude towards the security element, 7 of the 31 respondents (23%) still expressed their concern of someone stealing the phone and being able to misuse it. Despite the fact that majority of the respondents expressed positive opinion regarding authentication with the security elements, there were still 21 respondents out of the 79 (27%) who had a negative attitude and stated that they would not use the described authentication mechanism. The most common explanation for not using the security mechanism was the fear of losing the phone in the case of theft (11 statements). It was also often stated that the respondents do not want to save authentication information anywhere but rather keep it in their own memory (9 statements).

For both the responses of group A and group B, a one-sample t-test between proportions was performed to determine whether there were significantly more those who would be ready to use authentication with built-in security element (63%) than those who would not be ready to use it (27%). The t-statistic was significant at the 0,01 critical alpha level, as t(78)=3,646 and the corresponding one-tailed probability p=0,0003.

Related to mobile authentication utilizing a built-in security element, the respondents were also asked whether they would be ready to change their mobile phone to be able to use the described authentication mechanism. Majority of the respondents (45 out of 79, 57%) stated that they would not change their mobile phone to be able to use the security element for authentication. The respondents most commonly explained their attitude by expressing that they do not want the security element to steer their choice of mobile phone. Some respondents also stated that they did not see the security element to bring enough added value so that the respondents would change their mobile phone to be able to utilize it. 22 of the 79 respondents (28%) were somewhat more positive in their responses and stated that they would probably change their mobile phone to be able to use authentication with security element. Most of these respondents, however, stated that they would not change the phone just to get the new authentication feature, but would consider the option when the need to acquire a new phone will arise. The respondents also expressed that they would not be ready to pay much extra to get the security element in the phone. Only 7 of the 79 respondents (9%) stated that they saw authentication with security element enough valuable feature so that they would change their mobile phone when the feature would become available. A few of the respondents did not comment on the questions regarding the security element or stated that they were not sure about their opinion.

Also regarding this question, a one-sample t-test between proportions was performed to determine whether there were significantly more those who would not change their mobile phone to get to use the feature (57%) than those who had more positive attitude towards changing the phone (37%). The t-statistic was significant at the 0,05 critical alpha level, as t(78)=1,874 and the corresponding one-tailed probability p=0,0324.

5.6 User’s suggestions to improve perceived security

The respondents were asked to elaborate on things that they considered would enhance their perception of the security of a service. Overall, the respondents were not commenting the question widely and many of the respondents did not express their thoughts at all, but rather stated that they did not have ideas how perceived security of authentication could be improved.

Despite the generally low activeness in the responses, there were some of the respondents who elaborated their thoughts in the question. The most commonly noted aspect that the respondents thought would improve perceived security, was that there should be enough clearly visible information and signs of how the security is taken care of in the service (23 statements). Some of the respondents also expressed that there should be reliable and independent information available of the security level in mobile services that would be provided, for example, by some research institute (12 statements). According to the respondents, increased awareness would dispel suspicions that are based on mental impressions, and thereby perceived security would be affected positively. Some respondents also noted that security concerns could decrease as mobile authentication becomes more common and widely used indicating acceptance of other users.

A few respondents mentioned the positive effect of third-party security seals (e.g. McAfee Secure). They thought that having a verification sign of a trusted, independent company in the service would improve confidence in the security. Also indications of the involvement of trustworthy stakeholders such as banks or operators were mentioned as factors that improve perceived security. A few respondents even expressed that an official agency that would monitor the security levels of the services would give them a better feeling of security.

Some of the respondents expressed that their perception of the service security can be improved in the presence of one or more of the following: certain requirements for password complexity, indicator of password strength or regular requests to change password (7 statements). There were also some respondents who stated that their confidence in the security would increase if there would be a standardized authentication mechanism that would be available for all services and proved to be secure. A few respondents also generally commented that they wished development in the security features of mobile phones in order to feel more confident. Some more exceptional solutions that would increase confidence in the security of a service were also suggested, as a few of the respondents mentioned utilization of biometric identification (e.g. voice analysis, fingerprint identification or iris scan) in the services.

6 Synthesis

This chapter summarizes the findings from the empirical study of thesis and presents a synthesis of this thesis' results and the literature review on the related research. Firstly, the chapter presents some background information of both the literature review and the empirical study. Secondly, users' attitudes and general security perceptions are highlighted. Furthermore, the chapter covers factors that, according to this thesis, affect perceived security, as well as discussion on possibilities regarding new authentication solutions. The chapter is concluded by information of how perceived security affects intention to use mobile authentication.

6.1 Background

The related literature of this thesis consists of researches from various application areas such as e-commerce and mobile banking. However, none of the included studies explore perceived security of authentication directly. Therefore, the synthesis presented in this chapter connects the results from other application areas to the results from the empirical study of this thesis, and explores the possible similarities and differences. The empirical study of the thesis was realized as a web survey with 79 participants. The study participants were divided into two groups based on their backgrounds. Two-thirds of the respondents (n=52) had experience of authentication in mobile services, and therefore they were asked to answer the survey questions from the mobile authentication perspective (group A). On the other hand, the remaining third of the respondents (n=27) did not have mobile authentication experience, and thereby they were asked to base their survey responses on the experience of regular web services involving authentication and used with a PC or laptop (group B).

6.2 General attitudes and perceptions

The empirical study of this thesis shows that the general attitude towards new (mobile) services is more trusting than suspicious. Slightly over half of the survey respondents had a fairly trusting attitude, whereas approximately third of the study participants stated that they were fairly suspicious about new services. In the case of mobile authentication users, there were significantly ($p<0,05$) more of those users who were very trusting or fairly trusting than those who where fairly suspicious or very suspicious. The participants in the empirical study of this thesis expressed relatively similar attitudes towards new mobile services and new regular web services, as group A did not differ considerably from group B in their attitudes. Suspicious attitudes of users have been highlighted in related research as the users' confidence in technology has been claimed to be weak (Roboff & Charles, 1998; Pikkarainen et al., 2004).

According to the study results, the general perception of authentication security is good, as the vast majority of the participants (81% in group A and 96% in group B) stated that they considered the authentication as very secure or fairly secure. The proportions in both groups are statistically highly significant (p<0,01). Authentication in mobile services was perceived as less secure compared to regular web services, as group A expressed more of fairly insecure and less of fairly secure perceptions compared to group B. However, the difference between the groups was not statistically significant.

The survey study uncovered that the users' perceived security of authentication has not changed considerably. Only a slight change for the positive was noticed with the change being slightly more noticeable among the mobile authentication users. The empirical study revealed that the extent to which users think of security when they authenticate to services varies quite considerably. The proportions of the study participants thinking of security fairly much and fairly little were rather even and these statements constituted the majority in all responses.

6.3 Security mechanisms

The participants' awareness of the security mechanisms in services was found to be relatively weak, especially among the mobile authentication users with three-fourths of the group A being either fairly little aware, little aware or completely unaware. This proportion is statistically highly significant (p<0,01). Among the computer authentication users the corresponding proportion was a little over half of the group, indicating that with computers users seem to now a little better how the security has been taken care of, but still not very well. The quantitative findings are also supported by the qualitative data from the study, as many study participants expressed that the security mechanisms were rather or completely invisible for them. Mobile authentication users more frequently provided statements of the invisibility, indicating deficiencies in the security indications of mobile services requiring authentication. This finding is supported also by literature, as Botha et al. (2009) have highlighted the lack of provided security information as a factor that can negatively affect the security experience in mobile services. Yenisey et al. (2005) have highlighted that a service with well-implemented security may not show users clear indications of it. Perceived security of this kind of service can be weak, although objective security implementation is good.

Among those study participants who elaborated the visibility of underlying security implementation, most commonly mentioned signs of encrypted connection. Password inquiry, certificates and information dialogs of secured/unsecured connection were highlighted less frequently. The insufficiency of the security indications in mobile services is also supported by the fact that mobile authentication users generally mentioned visible indications of security less frequently than computer authentication users.

The empirical study reveals that although the security mechanisms are relatively invisible for the users and they are rather unaware of how the security is being taken care of (especially group A), the users still considered the observed security mechanisms to largely affect perceived security with over 60% of the both groups A and B rating the effect as either great or fairly large. In the case of group A, this proportion is not statistically significant ($p<0,05$), although the probability is very close ($p=0,0551$). In the case on group B, the proportion is statistically significant ($p<0,05$). The importance of observed security mechanisms has been also discussed in the related research, as Linck et al. (2006) have presented that the level of objective security influences the level of subjective security, Pousttchi & Wiedemann (2007) have reported the positive effect of encrypted connection on perceived security, and Kim et al. (2010) have stated that user’s perception of the technical protection in the service affects perceived security strongly and positively. The significant and positive effect of safety mechanisms on trust has also been presented by Gefen et al. (2003) and Kim et al. (2010). The fact that users in the empirical study of this thesis were relatively unaware of the security mechanisms, considered them to have a rather remarkable effect, but still felt that authentication is fairly secure is an interesting, yet somewhat contradictory, observation.

6.4 Provided security information

Based on the results of the empirical study, it is clear that there are deficiencies in the provided security information, especially in mobile services. This was considered to weaken perceived security. The study participants frequently noted that they wished to have more clearly visible and comprehensive information available of how the security of authentication in the service has been taken care of. This statement was the most common among the directly expressed wishes of what would improve perceived security, which indicates the importance of the finding. Also related research has identified security statements informing and assuring the users of the security to be important in improving both perceived security (Linck et al., 2006; Lim, 2008; Kim et al., 2010) and trust (Mukherjee & Nath, 2003; Lim, 2008). Salisbury et al. (2001) have suggested that providing the user with information of the taken security actions every time the user is asked to enter sensitive information could enhance perceived security.

The findings from the empirical study indicate that many users are not aware of the security in mobile services, and due to that perceived security is currently mostly based on mental impressions, which causes suspiciousness. Users' weak understanding of security risks has been highlighted also in the related research by Roboff & Charles (1998). According to the statements of this thesis' study participants, there is a clear need for reliable, independent information of the security in mobile services to be provided for the users (e.g. by research institutes).

6.5 Service usage experience

In the empirical study, the effect of past experience from the usage of mobile services or regular web services was discovered to have a considerable effect on perceived security. More than half of the study participants (56%) highlighted the effect in their survey responses. This proportion is significantly larger (p<0,01) than the proportion of users stating that usage experience has no effect on perceived security.

Additionally, the results regarding the general perception of authentication security showed that active mobile authentication users perceived the security to be better compared to mobile authentication users on average, indicating the positive effect of increased experience on perceived security. The past service experience was, for example, stated to help in recognizing the security risks and to increase the feeling of comfort as the services become more familiar. The effect of past experience has also been discussed in the related research. Bauer et al. (2005a) have suggested that lack of previous experience of new services can cause increased perceived risk. Shin (2010), in turn, has highlighted the positive effect of user expertise on perceived security. On the contrary, the related research has also pointed out that experience can also cause increased carefulness leading to decreased perceived credibility (Wang et al., 2003; Ong et al., 2004).

6.6 Positive and negative experiences

The results of this thesis' empirical study revealed that previous positive and negative experiences from certain services have a considerable effect on perceived security as users start using new services. 50% of the group A and 59% of the group B stated that past positive or negative experiences affect either greatly or fairly much. However, the proportion of respondents rating the effect great or fairly large does not statistically significantly differ from the percentage of other responses neither in the case of group A nor group B. Still, the large percentages show the importance of own past experiences. The negative experiences were generally considered to increase suspiciousness, whereas positive experiences were considered to increase confidence in the security of services. It was noticeable that negative experiences seemed to have stronger effect than positive experiences that seemed to be considered as a default more than something that would improve perceived security.

Many of the study participants noted that the past positive and negative most strongly affect to services that are made by the same company as the service from which the experiences originate or to services that highly resemble the service being the source of the experiences. Also related research has suggested that past positive and negative experiences affect perceived security. According to Miyazaki and Fernandez (2001), users with positive previous experiences are likely to continue use in the future, as the perceptions of security risks decline while the amount of positive experiences increases. Literature has also highlighted that positive experiences both decrease perceived risk and increase trust (Pavlou, 2003; Lim, 2008)

6.7 Experiences and recommendations of other people

According to the empirical study of the thesis, the experiences and recommendations of friends and acquaintances have even more considerable effect on perceived security than own experiences. 65% of the mobile authentication users and 59% of the computer authentication users stated that the experiences of others affect perceived security either greatly or fairly much. The proportion is statistically significant (p<0,05) for group A, but not for group B.

Also related research includes statements that the opinions of people who are important to the user affect the user's intention to engage in behavior, especially in the case of new technological phenomena (Vijayasarathy, 2004). Besides hearing experiences and recommendations from friends, the empirical study of this thesis also revealed that many users search for other users' experiences from Internet forums, for example. Both Jarvenpaa et al., 2000 and Shneiderman (2000) encourage providing references from past and current users in the service by showing citations of positive customer feedback. Furthermore, the importance of others' opinions for users was supported by the empirical study, as the participants stated that the confidence in security is improved when certain services or solutions become widely used among users, as this indicates acceptance of others.

6.8 Visual appearance and content

The empirical study of the thesis explored the effect of visual aspects on perceived security, and revealed that a vast majority of the study participants thought that the visual appearance of service affected perceived security. The study discovered certain characteristics that improve or decrease the confidence in security. The positive visual characteristics include

- Clearness and simplicity of the layout,
- Professional appearance,
- Correctness and formality,
- Visually pleasant, well-groomed and modern appearance,
- Use of quiet colors, and
- Logos of well-known and trustworthy companies.

The highlighted visual characteristics were, for example, stated to indicate that the service provider has invested effort to the service, also from the security perspective. Furthermore, the study participants mentioned certain content-related aspects that improve perceived security:

- Providing essential information about the security implementation to the user,
- Making contact information of the service provider easily available, and
- Showing proof of physical place of business provided that it exists.

In the literature, Shneiderman (2000) has highlighted that good design can enhance users' trust, and therefore attention should be paid to the structure of the service as well as the content. According to the empirical study, the negative visual characteristics that decrease perceived security include

- Ambiguous and disorganized appearance,
- Amateurish appearance,
- Clumsy appearance that indicates very quick and negligent implementation,
- Excessive advertisements
- Distracting content such as flash videos and unnecessary images,
- Poor quality of images and graphics,
- Strange color choices, use of glaring colors and excessive color use,
- Unfamiliar logos, and
- Unusual fonts.

Furthermore, the content-related negative aspects include

- Careless and flawed text and content,
- Mixed use of languages, and
- Use of odd and unfamiliar terminology.

The mentioned negative characteristics were, for example, claimed to imply that the service provider does not have the required competence to implement a secure service, does not want to invest effort in a secure implementation, or tries to hide something. In the related research, Vijayasarathy (2004) has discussed the significance of the visual aspects and the content of service for users, stating that poorly designed interfaces, confusing page layouts and outdated information are likely to cause frustration among the consumers. Relating to the negative effect of careless and flawed content, the importance of information quality for trust has been presented by Kim et al. (2008). According to the authors the information quality strongly and positively affects trust.

It was noticeable in the results of the empirical study that the negative aspects were commonly commented more emphatically and often before the positive aspects, indicating a more considerable effect of negative factors compared to the positive ones. The statements of some of the study participants that positive characteristics are expected to be a default support this assumption.

6.9 Ease-of-use and usability

The findings from this thesis' empirical study suggest that many users consider ease-of-use and usability as factors that affect perceived security. In addition to the few direct statements of the positive effect of ease-of-use and usability, many study participants highlighted aspects related to them. According to the statements, the service has to

- Be fluent and workable,
- Follow common conventions,
- Have an interface that is optimized for mobile phone
- Provide information of the consequences of performed actions and the practices of handling the confidential data,
- Provide clear use instructions and comprehensible terms of use, and
- Provide troubleshooting information when needed

On the other hand, uncommon design solutions, inconsistencies and obvious design flaws should be avoided as they have negative effect on perceived security. Related research has also discussed the effect of ease-of-use and usability on perceived security and the related constructs. Linck et al. (2006) have stated that convenience and ease-of-use positively affect perceived security. Casaló et al. (2007), in turn, have claimed that usability directly and significantly affect trust, and that perceived usability positively affects perceived security by improving comprehension of the tasks and content and making users feel more comfortable. Furthermore, the literature provides evidence of the significant effect of perceived ease-of-use on trust (Gefen et al., 2003) as well as perceived credibility (Wang et al., 2003; Ong et al., 2004).

The finding related to the positive effect of following common conventions has also been discussed in the literature as some authors have stated that an interface that complies with common conventions and situational norms is likely to increase trust of the users (Gefen et al., 2003; Gu et al., 2009). According to the findings of this thesis' empirical study, use of common conventions in the design improves perceived security through facilitating navigation and increasing the user's feeling of familiarity. Also the optimization of user interface for mobile phone has been mentioned in the literature, as Coursaris & Hassanein (2002) have suggested that content needs to be adapted to suit mobile devices. Furthermore, the finding of the need for providing information about the consequences of actions is supported by the related research, as Bauer et al. (2005a) state that uncertainty of the consequences of a decision or an action causes increased perception of riskiness.

Despite the recognized influence of ease-of-use and usability on perceived security in both the empirical study of this thesis as well as the related research, the empirical study discovered that excessive ease-of-use can also affect perceived security negatively. Many study participants highlighted that authentication should be complex enough so that it feels secure. However, it was also noted that excess complexity could cause frustration and weak usability, and therefore a balance between complexity and usability is essential in designing an authentication procedure that would be well-accepted by users. In the related research, Vijayasarathy (2004) has commented the negative effect of excessive complexity by stating that complicated navigational structures as well as complex checkout procedures may cause frustration for the users. Examining the comments of the participants in this thesis' study, it seems that the respondents most commonly refer to process-related aspects such as additional phases and confirmations as they discuss complexity. The related research suggests that the amount of money involved determines the need for complexity so that users prefer ease-of-use in the case of small payments but, due to security concerns, accept a more complex procedure when more money is involved (Mallat et al., 2004; Bauer et al., 2005b).

6.10 Authentication provider

The participants of the empirical study of this thesis were divided almost evenly to those who thought that there was a difference in the perceived security depending on whether a third-party company or the service provider itself provided the authentication, and to those who did not see difference in perceived security. User more often considered third-party authentication by a well-known company as secure compared to authentication by the company providing the service where authentication takes place. Two-thirds of the study participants expressed that they perceive the security of a certain third-party authentication similarly regardless of the service where it is utilized, whereas third of the participants stated the opposite (i.e. perceived security of the same third-party authentication can vary depending on the service where it is utilized). The difference between the proportions is statistically highly significant (p<0,01) for group A and statistically significant (p<0,05) for group B. A rather significant amount of users, who expressed the difference in security perception, might indicate that many users do not perceive a third-party authentication as a clearly separate element in the service, but form the perception of security based on the whole service.

The empirical study of this thesis uncovered that third-party security seals can be helpful in improving perceived security, as verification by a trusted company with security expertise seems to positively affect perceived security of some users. Furthermore, indications of the involvement of other trustworthy stakeholders such as banks and operators are likely to have positive effect on perceived security. The positive effect of utilizing third-party actors has also been mentioned in the literature**,** as third-party certification has been identified as a factor affecting perceived security (Linck et al., 2006) and trust (Shneiderman, 2000), and Kim et al. (2008) have stated that the use of third-party seal reduces the risk perceived by the user. Bauer et al. (2005b), in turn, have claimed that trusted third party actors and trust-intermediates could be effective in reducing perceived riskiness, and Goeke & Pousttchi (2010) have stated that trust can be improved by being proved by an independent institution. Jarvenpaa et al. (2000) recommends collaboration with companies that already have an established customer reputation.

6.11 Brand and reputation

The empirical study of this thesis uncovered that brand name and reputation of the authentication provider considerably affect perceived security, as the vast majority of respondents (85%) in both the group A and B considered the effect as great or fairly large. The proportion is statistically highly significant (p<0,01) for both groups A and B. This finding is supported also by the related research. The positive effect of strong brands on trust has been highlighted by Shneiderman (2000) and Yenisey et al. (2005). Furthermore, many authors have suggested that reputation directly and significantly affect both users' trust and perceived risk (Zucker, 1986; Doney & Cannon, 1997; Jarvenpaa et al., 2000; Ba & Pavlou, 2002; Pavlou, 2003; Casaló et al., 2007; Kim et al., 2008).

The study of this thesis uncovered that banks are widely considered as trustworthy authentication providers (half of the participants commenting). Furthermore, the study participants clearly expressed their preference for large, well-known and widely recognized companies. Finnish actors received the most trust in the study, but also well-known foreign companies such as Google and PayPal were highlighted as trustworthy service providers. The fact that users commonly consider banks as trustworthy actors has also been highlighted in the related research (e.g. Roboff & Charles, 1998 and Pikkarainen et al., 2004). The positive effect of large perceived company size, on the other hand, has also been confirmed by the literature. It has been claimed that large organizational size positively affects trust by indicating that a lot of other consumers trust the organization, the company has invested a lot of resources in the business, and it is also a signal that the company should have the necessary expertise and resources. (Doney & Cannon, 1997; Chow & Holden, 1997; Jarvenpaa et al., 2000).

6.12 Use context

The effect of use context on perceived security was found out to be considerable, as more than half of the users in both the group of mobile authentication users (63%) and the group of computer authentication users (52%) highlighted the effect of use context. In the case of group A, the proportion is statistically highly significant (p<0,01). The higher percentage among the mobile authentication users may be due to the fact that users of mobile services are more likely to encounter situations where security concerns arise. Most commonly the concerns were related to the possibility of losing the phone due to theft or someone spying on the passwords. In the related research, Botha et al. (2009) have stated that mobile devices are by their nature more vulnerable to security threats such as theft or accidental loss, and this brings users security concerns. The participants of empirical study also frequently expressed their suspiciousness towards the security of data transfer in mobile network and wireless connections in general. The weak security of open wireless networks also received attention in the both respondent groups. The users' suspiciousness towards wireless connections has also been highlighted in the related research, as Kindberg et al. (2004) has stated that many users instinctively consider docked, physical connections more secure than wireless connections.

6.13 Device

As the factors affecting perceived security were explored in the study, the effect of device was noticed in the comparisons of results between the groups A and B. The differences of the groups A and B in the general perceptions of authentication security show that the device used for authentication affects perceived security, in a way that mobile device is perceived as the less secure option. The device effect was also noticeable in the responses regarding the awareness of the security mechanisms, experiences and recommendations of other people, and use context. However, the differences were not statistically significant.

The effect of the used device was also directly enquired in the empirical study. The results showed that 65% of mobile authentication users and 33% of computer authentication users considered computer as a more secure device for authentication compared to mobile phone. In the case of group A, the proportion is statistically highly significant (p<0,01), whereas in the case of group B, the proportion is statistically significant (p<0,05). Furthermore, the proportion of users preferring computer in the group A is statistically significantly higher (p<0,01) than the corresponding proportion in the group B. The majority of computer authentication users (59%) did not see security differences between the devices. This findings suggests that users might have a neutral attitude towards the security in mobile services before they start using them, but as soon as users gain experience of mobile services and are able to compare the two devices, many of them start to consider mobile phone less secure than computer.

According to the empirical study, there are several reasons why mobile phone is considered as less secure than computer. Many study participants expressed reliability-related concerns such as breakdowns in the mobile Internet connection or freezing of mobile phone or service during the authentication. In the literature, Coursaris & Hassanein (2002) have commented on reliability issues by highlighting the importance of maintaining connection quality in mobile networks. According to the authors, breakdowns of connection can cause concerns of the personal data being lost. Losing critical information during, for example, financial transaction can have serious consequences, which can increase users' concerns. The effect of technical reliability on perceived security has been mentioned also by Linck et al. (2006). In the empirical study, the lack of virus protection and firewall was also considered to weaken the perceived security compared to computer.

Another significant reason for perceiving traditional computing safer than mobile phone is the fact that many users do neither have much experience of mobile use nor much information of the security level in mobile services, which causes suspiciousness via lack of knowledge. On the other hand, users have more experience of traditional computing, and the familiarity is likely to improve perceived security. The positive effect of familiarity has also been mentioned by Ba & Pavlou (2002) who claim that familiarity and repeated interaction affect users' trust on the services. Also Kim et al. (2008) have presented the effect of familiarity on trust.

Also physical characteristics of mobile phones (e.g. small screen size and poor writing capabilities) were highlighted to cause uncertainty via inconvenience, whereas many users felt more confident using a computer due to convenience. Some authors in the related research (e.g. Gillick & Vanderhoof, 2000) have discussed the serious limitations of the screen size and text input mechanisms of mobile devices, and it has been stated that due to convenience issues most users will continue using their home computer until the usability barriers of mobile devices are no longer an issue.

6.14 New authentication solutions

Besides exploring perceived security of currently utilized means for user authentication in mobile services and regular web services, the empirical study of this thesis also examined the users' attitudes towards new authentication solutions. The study enquired users' opinions of mobile authentication that would utilize a built-in security element of a mobile phone, enabling authentication in certain services. The results show that the attitudes of the study participants vary fairly much. Approximately fourth of the participants stated that they would use the authentication solution for all services. Around 40% of the participants, in turn, expressed their willingness to use the solution, but only with certain conditions (e.g. an additional password besides the security element) or in certain services that do not involve sensitive, personal information or money. Approximately fifth of the participants stated that they would not use the authentication solution in any case. The most common reason for careful and negative attitudes was the fear of losing the mobile phone in the case of theft, which already turned out to concern users as the effect of use context on perceived security was explored. Furthermore, many users expressed that they were not comfortable with the idea of storing authentication data inside mobile phone, but preferred their own memory for storing sensitive information. Despite some of the negative statements, the proportion of users who would be ready to use the authentication with built-in security element is statistically significantly higher ($p<0,01$) than the proportion of users not ready to use the feature.

The study uncovered that users were mostly (57%) unwilling to change mobile phone to be able to use the new authentication solution, as it was not considered to be enough valuable feature to steer the phone purchase. Some of the study participants (28%), in turn, expressed their willingness to consider the security element as an important feature when a need to acquire new phone arises, but extra cost was not justified in the respondents' opinion. Only a minority of participants (9%) stated that they considered the security element so valuable that they would change their phone to get the feature as the solution becomes available. The proportion of users not willing to change the phone is statistically significantly higher ($p<0,05$) than the proportion of users with more positive attitude.

Despite the generally negative comments related to the authentication with built-in security element, there were some users who directly wished a standardized authentication mechanism that would be available for all mobile services and proved to be secure. These statements indicate that there is a need for a centralized authentication mechanism, but it is essential to make sure that users are assured of the security of the solution. Therefore, users could also accept the mobile authentication solution utilizing the security element if they would be well informed of how the security of the solution has been assured. Dispelling the security concerns, especially regarding services involving money, is essential as the concerns were clearly highlighted in the study.

Some of the study participants suggested also more exceptional solutions for authentication that would be perceived secure. These solutions were based on biometric identification (e.g. voice analysis, fingerprint identification or iris scan). These suggestions might not be as feasible alternatives for authentication as the security element, since biometric identification can, for example, affect device prices more than the security element. Many of the users in the empirical study clearly expressed that extra cost is not easily justified.

6.15 Intention to use mobile authentication

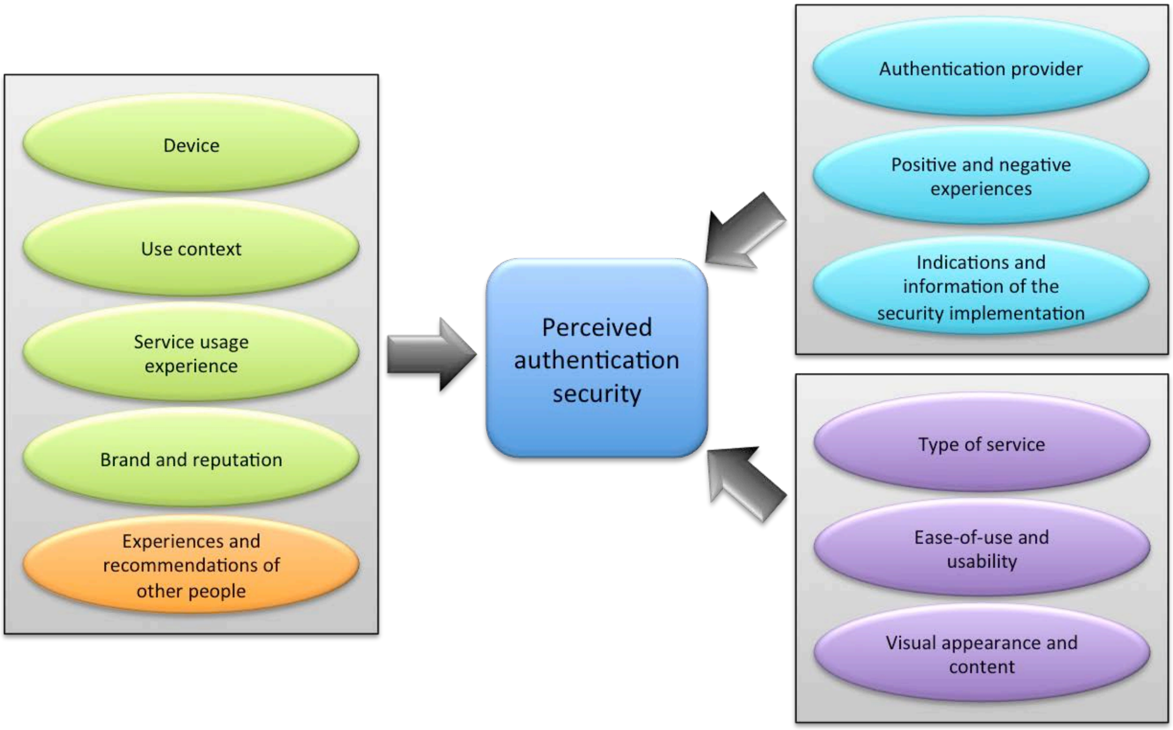
The literature review on the related research showed that perceived security and the related constructs have been identified as factors that significantly affect the intention to use a service either directly (Jarvenpaa et al., 2000; Miyazaki & Fernandez, 2001; Salisbury et al., 2001; Pavlou, 2003; Gefen et al., 2003; Wang et al., 2003; Ong et al., 2004; Liu et al., 2005; Casaló et al., 2007; Mallat, 2007; Kim et al., 2008; Shin, 2010) or via attitude towards use (Jarvenpaa et al., 2000; Vijayasarathy, 2004; Hsu & Chiu, 2004; Bauer et al., 2005a; Shin, 2010; Schierz et al., 2010). The empirical study of this thesis showed that perceived security also affects the users' intention to use authentication. However, it was noticed that the nature of the service where the authentication takes place has a considerable effect on how important the users consider the security to be, and how the perceived security affects the use intention. Also related research has pointed out this fact, as Coursaris & Hassanein (2002) state that users become increasingly concerned of the safety of the information transferred over a wireless network as the degree of interaction and the sensitivity of the exchanged information increases.

The study participants were most concerned of the security when money is involved, as almost all of them highlighted money in their survey responses. In the case of almost half of the mobile authentication users (group A), the security concerns were so considerable that the respondents stated they are not using online banking services with their mobile phone. Some also expressed that they were not willing to make large purchases with mobile phone. This has been highlighted also in the related research, as Coursaris & Hassanein (2002) have stated that consumers are unlikely to purchase expensive items online, and that they are even more hesitant toward purchases with mobile phone. The studies in related research that have identified perceived security as an important determinant of use intention in the contexts of banking services (e.g. Wang et al., 2003) and electronic commerce (e.g. Vijayasarathy, 2004) are supported by the findings of the empirical study of this thesis.

The study of this thesis reveals that many users are also concerned of security in services involving sensitive, personal information (e.g. social media and email). However, these statements were considerably less frequent than those related to money, and some of the study participants also directly stated that security in these services was not crucial. Additionally, security was not expressed to be a reason for not using these services with mobile phone, as was the case for many when money is involved. The studies in related research focusing on social media (e.g. Shin, 2010) and stressing the importance of perceived security for use intention are therefore not as strongly supported by the findings of this thesis as the studies regarding online banking and electronic commerce.

In this thesis' empirical study, it was found out that security is not an important factor in services related to entertainment purposes (e.g. gaming, news, forums). In the related literature, Coursaris & Hassanein (2002) have claimed that security of less personal and interactive services such as weather notifications does not bother users. Although almost half of the mobile authentication users in the empirical study expressed their unwillingness to use mobile banking services, still half of the mobile authentication users stated that perceived security does not affect whether they use a mobile service or not. However, some study participants stated that they prefer computer to mobile phone if they have the possibility to choose the device used for authentication.

To conclude Chapter 6, Figure 27 summarizes all of the factors that affect perceived authentication security according to the findings of this thesis. Additionally, the color-coding indicates the quality of findings in the case on mobile authentication users. The factors marked with green color were found to be statistically highly significant ($p<0,01$), and the factor marked with orange color was found to be statistically significant ($p<0,05$). The factors marked with light blue color were found to be very important although statistical significance was not reached (for indications and information of security implementation the statistical significance was almost attained). The factors marked with purple color were identified from purely qualitative data and calculations of statistical significance were therefore not possible. Despite lacking the statistical proof of significance, it is obvious, based on the results, that these factors are very important determinants of perceived authentication security.



Device
Use context
Service usage experience
Brand and reputation
Experiences and recommendations of other people
Perceived authentication security
Authentication provider
Positive and negative experiences
Indications and information of the security implementation
Type of service
Ease-of-use and usability
Visual appearance and content

Figure 27. Factors that affect perceived authentication security

7 Conclusions

This thesis explored perceived security of mobile authentication, a topic that has not been previously studied directly. The examination covered both literature review on the related research as well as an empirical study that was realized as a web survey. The findings show that perceived security of mobile authentication is important for users, and it can considerably affect the intention to use certain mobile services. The examination of this thesis provides evidence to the assumption that security concerns related to mobile services are more pronounced than those related to the more traditional services used with a computer.

Firstly, this chapter presents answers to the three first research questions of this thesis. Secondly, the fourth research question is answered by presenting recommendations for taking perceived security into account in the designs. Finally, presenting a few important final words concludes the chapter.

7.1 Answering the research questions

Within this thesis, information has been gathered both with literature review and an empirical study. This information has been used for seeking answers to the research questions of the thesis. This subchapter concludes the answers to these questions.

Rq1 How do Finnish mobile phone users currently perceive the security of mobile authentication?

According to the results of the empirical study, Finnish users generally perceive the security of mobile authentication as fairly secure. However, this does not hold true for all mobile services. The findings of this thesis show that half of the users do not use mobile banking services due to security concerns, which implies a considerable lack of perceived security in the services dealing with money. The results regarding users’ attitudes towards new mobile services reveal that, from the statistical perspective, significantly more users have trusting attitude than suspicious attitude. However, the great number of users with suspicious attitude clearly shows that users certainly have doubts related to security of mobile services.

Rq2 How does perceived security of mobile authentication differ from perceived security of authentication in regular web services?

Mobile services are still relatively new as a phenomenon, meaning that users naturally have less experience of them compared to services used in the traditional computing environment. The findings of this thesis indicate that users, indeed, have a more careful attitude towards mobile services. Consequently, statistically significant majority of the users with mobile authentication experience consider authentication more secure with computer than with mobile phone. Mobile authentication users also expressed this opinion significantly more emphatically than computer authentication users. Also the examinations regarding the determinants of perceived security indicate that perceived security of mobile authentication is considered to be weaker than that of authentication in regular web services. However, these differences are not statistically significant. Still, it must be highlighted that the users of the empirical study do not represent average Finnish users due to their technological background, and therefore it is reasonable to assume that the difference might have been larger with users closer to the average.

Rq3 What factors affect perceived security of mobile authentication?

This thesis explored the factors that contribute to the formation of perceived security in mobile authentication. It was discovered that perceived security is a relatively complex phenomenon that is affected by various factors. A total of 11 factors were identified, and they are listed below so that statistically highly significant factors are mentioned first, followed by statistically significant factors and other factors of great importance. The factors that were identified from purely qualitative data are listed last, but this does not indicate that they would be of less importance.

1. **Device.** The examination shows that device used for authentication affects perceived security considerably. A statistically highly significant majority of users perceive the authentication to be more secure with computer.
2. **Use context.** The findings show that context of use affects perceived security of mobile authentication. The effect is statistically highly significant. The most typical reason for concerns related to mobile use context is the possibility of losing mobile phone due to theft.

3. **Service usage experience.** The findings suggest that the amount of experience of using mobile services has a considerable, positive effect on the perceived authentication security. The effect is statistically highly significant.
4. **Brand and reputation.** The findings show that brand and reputation both significantly affect perceived security. The effect is statistically highly significant. Users trust banks and large, well-known companies the most.
5. **Experiences and recommendations of other people.** The examination of this thesis uncovered that experiences and recommendations of other people have a statistically significant effect when user forms conception of the security of mobile authentication. Besides the information heard from friends and acquaintances, users also give value to other people's experiences that they find from the Internet, for example.
6. **Indications and information of the security implementation.** According to the findings, users are fairly unaware of how security has been taken care of in mobile authentication, and for many users the security mechanisms are rather or completely invisible. For a significant majority of users, the visibility of security mechanisms is an important factor that affects perception of authentication security. Additionally, assuring statements of the means used to guarantee the security of authentication are important for many users.
7. **Past positive and negative experiences.** In the light of the elicited information, it can be stated that past positive and negative experiences of mobile services that involve authentication considerably affect perceived security. The findings suggest that negative experiences have a stronger effect than positive experiences.
8. **Authentication provider.** The results of empirical study show that half of the users perceive security of authentication differently depending on whether a third-party company or the service provider itself provides the authentication. The users seemed to prefer third-party authentication more of the two alternatives. Furthermore, third of users perceive the security of third-party authentication differently depending on the service where it is utilized.
9. **Visual appearance and content.** The findings show that visual aspects and the content of the service affect perceived security to a great extent. Various

characteristics having either positive or negative effect were identified. Negative aspects seem to have more effect than positive ones.

10. **Ease-of-use and usability.** It was discovered that both ease-of-use and usability positively affect perceived security in mobile authentication. However, the findings show that excessive ease-of-use can also negatively affect perceived security. Therefore, users are willing to accept some complexity in the authentication procedure to feel secure.
11. **Type of service.** The examination revealed that the type of service where authentication takes place affects users' perception of security. Users also consider security to be of varying importance depending on the service. Security is most important in services that involve money, whereas users are least concerned of security in entertainment services.

7.2 Recommendations

This subchapter answers the fourth research question (**Rq4** How to improve perceived security of mobile authentication?). Based on the findings of this thesis, certain recommendations can be made to help designers and developers of new solutions in taking perceived security into account, as well as developers of current solutions to improve perceived security of existing designs.

1. Provide users with clear and comprehensible indications of the security implementation of authentication. Also credible and convincing statements of how the security of authentication has been taken care of are recommended to assure users of the security. These matters are especially important in the case of services involving money.
2. In points where user has to make decisions regarding submitting personal data, provide user with clear and comprehensible information of how the confidential user information will be transferred and what will happen next.
3. Users value other people's experiences and recommendations when evaluating perceived security. Utilize this fact by providing positive user comments and feedback in the service

4. Strong brands are effective in conveying trustworthiness to users. Collaborate with trustworthy stakeholders that already have a good reputation (e.g. banks), and provide indications of the involvement of these actors to users. Additionally, utilizing well-known third-party seals in the service can be useful to increase credibility and improve the users' perception of the authentication security.
5. The visual appearance of the service should be considered carefully to maximize the number of positive security indicators and minimize the number of negative security indicators.
    a. The appearance should be modern, clearly organized, and it should contain only necessary information and elements. Use of quiet colors is advisable. Correctness and formality are also important characteristics in conveying a message of a professional service provider that the users will trust.
    b. The layout should be optimized for mobile use.
    c. It is advisable to have clearly visible logos of well-known companies with good reputation.
    d. The number of advertisements and other distracting content should be minimized. The necessary advertisements should be as little disruptive as possible and they should preferably be connected to companies with good reputation.
    e. Pay attention to color and font choices. Avoid strange and unusual colors as well as glaring colors. Use only typical fonts.
6. Follow common conventions when designing the visual appearance and functionality. This increases the feeling of familiarity and thereby makes users feel more comfortable. In the design of completely new ways of authenticating, try to preserve some familiar elements from the more conventional solutions.
7. Take care of the information quality of the content. Use proper language, be consistent and avoid use of odd or unfamiliar terminology.
8. Pay attention to the usability of the solution and make use fluent. However, especially in the case of services involving money, certain complexity in the form of extra steps and confirmations is advisable to improve perceived security.

9. Consider the fact that users are widely concerned of phone theft. Develop means to protect the user in the case of theft, and assure users of the security of the solution.
10. Remember that perceived security is not only affected by the authentication part of the mobile service. The other elements in the service affect perceived security as well. Therefore, care should be taken in the design process so that the whole service conveys a trustworthy message, not only the authentication procedure. This fact can cause challenges in the case of independent authentication solutions that will be utilized in numerous services, since the provider of the authentication solution cannot affect much the design of the service.
11. Increasing users’ awareness of the security of mobile authentication and mobile data transfer is essential, so that perceived security would be formed from the basis of knowledge rather than mental impressions. To maximize the credibility and assuring value of the information, neutral and independent stakeholders should provide it.

The examination conducted within this thesis has clearly shown that developing objectively secure authentication solutions does not alone guarantee user acceptance. The user’s subjective perception of security is the crucial factor in determining the intention to use services, and therefore assuring users of the authentication security is of utmost importance. The thesis has highlighted that perceived security is a complex concept with various affecting factors. Thus, enough time to thoroughly address all necessary aspects should be reserved from the development process.

8 Discussion

The examination of this thesis was targeted on the mobile authentication, a topic that has not been previously studied in the related research as a separate subject. Therefore, the work done within this thesis can be claimed to have novelty value. Many studies have been conducted related to services that involve user authentication as one element (e.g. electronic commerce and online banking), but they have explored perceived security or the other related constructs in a general sense, with respect to the whole service. Despite the fact that a more targeted approach of this thesis enabled gathering rather detailed information of perceived security in mobile authentication, it also revealed that many users do not consider authentication as a separate element in the service, but rather form the perception of authentication security based on the whole service. This is an important finding from the perspective of development of new centralized authentication solutions. However, it has been left unnoticed in the more general examinations of the related research.

Many of the studies in related research have not studied perceived security or the other related constructs in a targeted manner, but rather as one element contributing to the user acceptance. As the studies have covered also other factors of user acceptance, they have not been able to dive deep into the topic, but have left the examination to a fairly superficial level. This can be considered as one drawback of utilizing TAM model as the basis for research frameworks. Since the main objective of this thesis was to thoroughly study perceived security, it was possible to concentrate on exploring the topic in more depth and gain a better understanding of the factors contributing to the construct.

8.1 Validity and reliability of the study

Certain facts must be noted when evaluating the validity and reliability of the examination of this thesis. Firstly, the participants of the empirical study represent only a limited and narrow sample of all potential users of mobile authentication in Finland. Due to the technology-oriented background and young average age of the participants, it has to be considered that wide generalizations of the results regarding users’ attitudes and current perceptions of authentication security may not be reliable. It remains a topic to be further studied whether users closer to the Finnish average would differ in their attitudes and perceptions from the technologically oriented users of the empirical study. Nevertheless, it needs to be highlighted that the technologically oriented users were probably more able to comment on certain matters, which was beneficial in determining the factors that contribute to perceived security as well as finding out how perceived security could be improved. Additionally, technology-oriented user group enabled getting a large number of users that had experience of mobile authentication and were therefore able to comment on it. With a less technologically oriented user group this would not have necessarily been possible.

Secondly, it needs to be highlighted that there is a minor risk that some of the survey respondents with no mobile authentication experience were not answering the questions as was guided. When experience of mobile authentication was enquired, it was instructed in the subsequent question that those who do not have mobile authentication experience should respond to all of the remaining survey questions by thinking of their experiences of authentication in regular web services used with a computer. The remark was not repeated in the remaining questions, since it was assumed that people would remember the instruction for the rest of the survey. Thus, there is a possibility that some users may have forgotten the instruction by the time they were answering the last questions. However, when conducting the analysis of the collected material, no clear indications of the presented behavior were noticed. In addition, the risk is mitigated by the fact that the majority of users with no mobile authentication experience were also not using mobile Internet services in general, which can be considered to have increased the probability of the computer authentication users answering all of the survey questions as was instructed.

Finally, it must be noted that the comparisons of the differences between mobile authentication and computer-based authentication might have been more reliable if the users with mobile authentication experience had answered the questions by evaluating both the case of mobile authentication and computer-based authentication. This procedure would have resulted in a more direct comparison. However, it was not a viable option, since the survey was fairly long and time-consuming, and it would have been unfair for the majority of the respondents (i.e. users with mobile authentication experience) to be required to answer more questions than those of the respondents who did not have mobile authentication experience.

8.2 Further development

This thesis explored perceived security of mobile authentication in general, without specifying the examination to any particular authentication solution. The work has helped in forming a comprehensive conception of the subject that has not been widely studied before, and has made a number of suggestions on how perceived security can be taken into account when designing new mobile solutions. In future, it would be reasonable to develop prototypes that could be used to explore the topic with respect to certain particular solutions for mobile authentication. This way, a more precise and targeted examination of the impacts of certain design solutions on perceived security could be performed.

A considerable proportion of the related research has explored perceived security as one factor that contributes to user acceptance, and has utilized TAM model as the basis of research frameworks. Perceived security has not been directly connected to user experience in neither the thematically related research of this thesis nor the user experience research. However, the new standard definition of user experience (ISO 9241-210:2010) points out that user experience includes all of the user's perceptions and attitudes. Nevertheless, the definition is very wide. It can also be highlighted that Morville's (2004) honeycomb framework includes credibility as one determining factor of user experience. Although credibility does not equal with perceived security, it can be seen as one point where making the connection between user experience and perceived security could start. Considering the fact that many of the new mobile services involve confidential data that needs to be secured, perceived security is an important aspect that should be taken into account in the user experience design.

References

Ajzen, I. (1985). From intentions to actions: a theory of planned behavior. In Kuhl, J. & Beckmann, J. (Eds), *Action Control: From Cognition to Behavior*, Springer-Verlag, New York, NY, pp. 11-39.

Ajzen, I. & Fishbein, M. (1980). Understanding Attitudes and Predicting Social Behavior. Prentice-Hall, Englewood Cliffs, NJ.

Androulidakis, I. & Kandus, G. (2010). Trends in users' security perceptions regarding mobile phone usage. In *Proceedings of the 14th WSEAS international conference on Communications (ICCOM'10),* Mastorakis, N. E., Mladenov, V. and Bojkovic, Z. (Eds.). World Scientific and Engineering Academy and Society (WSEAS), Stevens Point, Wisconsin, USA, pp. 63–69.

Ba, S. & Pavlou, P. A. (2002). Evidence of the effect of trust building technology in electronic markets: Price premiums and buyer behavior, *MIS Quarterly*, 26, (3), pp. 243–268.

Bagozzi, R. P. (2007). The legacy of the technology acceptance model and a proposal for a paradigm shift. *Journal of the Association for Information Systems,* 8, (4), pp. 243–254.

Baier, A. (1986). Trust and Antitrust. *Ethics*, 96, (2), pp. 231–260.

Bauer, H. H. & Reichardt, T. & Barnes, S. J. & Neumann, M. M. (2005a). Driving consumer acceptance of mobile marketing: a theoretical framework and empirical study. *Journal of Electronic Commerce Research*, 6, (3), pp. 181–191.

Bauer, H. H. & Reichardt, T. & le, A. (2005b). User Requirements for Location Based Services. In *Proceedings of the IADIS International Conference E-Commerce 2005*, 2, pp. 211–218.

Botha, R. A. & Furnell, S. M. & Clarke, N. L. (2009). From desktop to mobile: Examining the security experience. *Computers & Security,* 28, (3-4), pp. 130–137.

Bouwman, H. & Carlsson, C & Molina-Castillo, F. J. & Walden, P. (2007). Barriers and drivers in the adoption of current and future mobile services in Finland. *Telematics and Informatics*, 24, (2), pp. 145–160.

Casaló, L. V. & Flavián, C. & Guinalíu, M. (2007). The role of security, privacy, usability and reputation in the development of online banking. *Online Information Review*, 31, (5), pp. 583–603. DOI: 10.1108/14684520710832315

Chari, S. & Kermani, P. & Smith, S. & Tassiulas, L. (2001). Security Issues in M-Commerce: A Usage-Based Taxonomy. In *E-Commerce Agents: Marketplace Solutions, Security Issues, and Supply and Demand* (Liu, J. and Ye, Y. Eds.), pp. 264–282. 1st Edition. Springer, Berlin.

Chau, P. Y. K. & Hu, P. J.-H. (2001). Information technology acceptance by individual professionals: a model comparison approach. *Decision Sciences*, 32, (4), pp. 699–719.

Chow, S. & Holden, R. (1997). Toward an understanding of loyalty: the moderating role of trust. *Journal of Managerial Issues*, 9, (3), pp. 275–298.

Clarke, N. L. & Furnell, S. M. (2005). Authentication of users on mobile telephones – a survey of attitudes and practices. *Computers & Security*, 24, (7), pp. 519–527.

Corritore, C. & Kracher, B. & Wiedenbeck, S. (2003). On-line trust: evolving themes, a model. *International Journal of Human-Computer Studies*, 58, pp. 737–758.

Coursaris, C. & Hassanein, K. (2002). Understanding M-Commerce: A consumer-centric model. *Quarterly Journal of Electronic Commerce,* 3, (3), pp. 247–271.

Dan, K. J. & Ferrin, D. L. & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk and their antecedents. *Decision Support Systems*, 44, pp. 544–564.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology, *MIS Quarterly*, 13, (3), pp. 319–340. ISSN: 0276-7783. Available online: http://www.jstor.org/stable/2634758.

Davis, F. D. & Bagozzi, R. P. & Warshaw, P. R. (1989). User Acceptance of Computer Technology: A Comparison Of Two Theoretical Models. *Management Science*, 35, (8), pp. 982–1003.

Doney, P. M. & Cannon, J. P. (1997). An Examination Of The Nature Of Trust In Buyer-Seller Relationships. *Journal Of Marketing*, 61, (2), pp. 35-51.

Friedman, B. & Kahn, P.H. & Howe, D.C. (2000). Trust Online. *Communications of the ACM*, *43,* (12), pp. 34–40.

Ganesan, S. (1994). Determinants of long-term orientation in buyer-seller relationships. *Journal of Marketing*, 58, (2), pp. 1-19.

Gefen, D. & Karahanna, E. & Straub, D. W. (2003). Trust and TAM in online shopping: an integrated model. *MIS Quarterly*, 27, (1), pp. 51–90.

Gillick, K & Vanderhoof, R. (2000). Mobile E-Commerce: Market Place Enablers and Inhibitors. A White Paper for the Smart Card Forum. Smart Card Forum Annual Meeting, September 25 – 28, 2000

Goeke, L & Pousttchi, K. (2010). A scenario-based analysis of mobile payment acceptance. *9th International Conference on Mobile Business*. DOI 10.1109/ICMB-GMR.2010.81

Gorlenko, L. & Merrick, R. (2003). No wires attached: Usability challenges in the connected mobile world. *IBM Systems Journal*, 42, (4), pp. 639–651.

Gruen, M. E. (2006). A Secure Low-Power Approach for Providing Mobile Encryption. *Journal of Computing Sciences in Colleges*, 21, (6), pp. 288–289.

Gu, J.-C. & Lee, S.-C. & Suh, Y.-H. (2009). *D*eterminants of behavioral intention to mobile banking. *Expert Systems with Applications*, 36, (9), pp. 11605–11616.

Hassenzahl, M. (2001). The Effect of Perceived Hedonic Quality on Product Appealingness. *International Journal of Human-Computer Interaction*. 13, (4), pp. 481–499

Hassenzahl, M. (2003). The thing and I: Understanding the relationship between user and product. In Blythe, M. A. & Overbeeke, K. & Monk, A. F. & Wright, P. C. (eds.). *Funology: From Usability to Enjoyment*, pp. 43–54. Kluwer Academic Publishers, Dordrecht. ISBN: 1-4020-1252-7

Hassenzahl, M. (2006). Hedonic, emotional, and experiential perspectives on product quality. In C. Ghaoui (ed.), *Encyclopedia of Human Computer Interaction*. Idea Group (2006), pp. 266–272.

Hassenzahl, M. (2010). *Experience Design: Technology for all the right reasons*. USA: Morgan & Claypool. 85 p. ISBN: 9781608450473

Hassenzahl, M. & Tractinsky, N. (2006). User Experience - a research agenda [Editorial]. *Behavior & Information Technology*, 25, (2), pp. 91–97.

Hassenzahl, M. & Law, E. & Hvannberg, E. (2006). *U*ser Experience: Towards a Unified View. In E. Law, E. Hvannberg, & M. Hassenzahl (Eds.), P*roceedings of the NordiCHI 2006 Workshop "User Experience: Towards a Unified View"* (pp. 1–3), Oslo, Norway, 14 Oct. 2006

Hsu, M.-H. & Chiu, C.-M. (2004). Internet self-efficacy and electronic service acceptance. *Decision Support Systems* 38, (3), pp. 369–381.

Hwang, R.-J. & Shiau, S.-H. & Jan, D.-F. (2007). A new mobile payment scheme for roaming services. *Electronic Commerce Research and Applications,* 6, (2), pp. 184–191.

ISO 9241-210. (2010). Ergonomics of Human System Interaction – Human-centred design for interactive systems. International Organization for Standardization, Geneva, standard. 32 p.

Jarvenpaa, S. L. & Lang, K.R. & Takeda, Y. & Tuunainen, V.K. (2003). Mobile commerce at crossroads: An international focus group study of users of mobile handheld devices and services. *Communications of the ACM*, 46, (12), pp. 41–44.

Jarvenpaa, S. L. & Tractinsky, N. & Saarinen, L. (1999). Consumer Trust in an Internet Store: A Cross-Cultural Validation. *Journal of Computer-Mediated Communication*, 5, (2).

Jarvenpaa, S. L. & Tractinsky, N. & Vitale, M. (2000). Consumer trust in an Internet store. *Information Technology and Management* 1, (1-2), pp. 45–71.

Kaasinen, E. (2005). User acceptance of mobile services – value, ease of use, trust and ease of adoption. Doctoral dissertation, VTT. VTT Publications 566. VTT, Espoo. Available online: http://www.vtt.fi/inf/pdf/publications/2005/P566.pdf

Karatzouni, S. & Furnell, S. F. & Clarke, N. L. & Botha, R. A. (2007). Perceptions of user authentication on mobile devices. In *Proceedings of the 6th Annual ISOneWorld Conference*, Las Vegas, USA, April 11–13.

Kim, C. & Tao, W. & Shin, N. & Kim, K.-S. (2010). An empirical study of customers' perceptions of security and trust in e-payment systems. *Electronic Commerce Research and*

Applications, 9, (1), pp. 84–95.

Kim, D. J. & Ferrin, D. L. & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision Support Systems*, 44, (2), pp. 544–564.

Kim, H. & Kim, J. & Lee, Y. (2005). An Empirical Study of Use Contexts in the Mobile Internet: Focusing on the Usability of Information Architecture. In*formation Systems Frontiers*, 7, (2), pp. 175–186.

Kindberg, T. & Sellen, A. & Geelhoed, E. (2004). Security and Trust in Mobile Interactions: A Study of Users' Perceptions and Reasoning. *UBICOMP 2004: Lecture Notes in Computer Science*, Volume 3205/2004, pp. 196–213, DOI: 10.1007/978-3-540-30119-6_12

Kleijnen, M. & Ruyter, K. D. & Wetzels, M. (2007). An assessment of value creation in mobile service delivery and the moderating role of time consciousness. *Journal of Retailing*, 83, (1), pp. 33–46

Laforet, S. & Li, X. (2005). Consumers' attitudes towards online and mobile banking in China. *International Journal of Bank Marketing*, 23, (5), pp. 362–380.

Law, E. L-C. & Roto, V. & Hassenzahl, M. & Vermeeren, A. & Kort, J. (2009). Understanding, Scoping and Defining User eXperience: A Survey Approach. *CHI '09 Proceedings of the 27th international conference on Human factors in computing systems.* DOI: 10.1145/1518701.1518813

Linck, K. & Pousttchi, K. & Wiedemann, D. G. (2006). Security Issues in Mobile Payment from the Customer Viewpoint. In Ljungberg, J. (Ed.), *Proceedings of the 14th European Conference on Information Systems (ECIS 2006).* Göteborg, Sweden 2006. pp. 1–11.

Lim, A. S. (2008). Inter-consortia battles in mobile payments standardisation. *Electronic Commerce Research and Application*, 7, (2), pp. 202–213.

Liu, C. & Marchewka, J.T. & Lu, J. & Yu, C.-S. (2005). Beyond concern – A privacy-trust-behavioral intention model of electronic commerce, *Information and Management*, 42, (2), pp. 289–304.

Mallat, N. (2007). Exploring Consumer Adoption of Mobile Payments - A Qualitative Study. *The Journal of Strategic Information Systems*, 16, (4), pp. 413–432.

Mallat, N. & Rossi, M. & Tuunainen, V. K. (2004). Mobile Banking Services. *Communications of the ACM*, 47, (5), pp. 42–46.

Mitchell, V.-W. (1999). Consumer perceived risk: conceptualisations and models. *European Journal of Marketing*, 33, (1/2), pp. 163–195.

Miyazaki, A. D. & Fernandez, A. (2001). Consumer Perceptions of Privacy and Security Risks for Online Shopping. *Journal of Consumer Affairs*, 35, (1), pp. 27–44. DOI: 10.1111/j.1745-6606.2001.tb00101.x

Mukherjee, A. & Nath, P. (2003). *A* Model Of Trust In Online Relationship Banking. *International Journal Of Bank Marketing*, 21, (1), pp. 5–15.

Ong, C.-S. & Laia, J.-Y. & Wang, Y.-S. (2004). Factors affecting engineers' acceptance of asynchronous e-learning systems in high-tech companies. *Information and management*, 41, (6), pp. 795–804.

Pavlou, P. A. (2003). Consumer Acceptance Of Electronic Commerce: Integrating Trust And Risk With The Technology Acceptance Model, *International Journal Of Electronic Commerce*, 7, (3), pp. 101–134.

Peter, J. P. & Tarpey, L. X. (1975). A comparative analysis of three consumer decision strategies. *Journal of Consumer Research*, 2, (1), pp. 29–37.

Pikkarainen, T. & Pikkarainen, K. & Karjaluoto, H. & Pahnila, S. (2004). Consumer acceptance of online banking: An extension of the technology acceptance model. *Internet Research*, 14, (3), pp. 224–235.

Pousttchi, K. & Schurig, M. (2004). Assessment of Today's Mobile Banking Applications from the View of Customer Requirements. *Proceedings of the 37th Annual Hawaii International Conference on System Sciences (HICSS'04)*, 7. Available online: http://doi.ieeecomputersociety.org/10.1109/HICSS.2004.1265440.

Pousttchi, K. & Wiedemann, D. G. (2007). What Influences Consumers' Intention to Use Mobile Payments? *Proceedings of the Global Mobility Roundtable*, Los Angeles, California, USA.

Roboff, G. & Charles, C. (1998). Privacy of financial information in cyberspace: Banks addressing what consumers want. *Journal of Retail Banking Services*, 20, (3), pp. 51–56.

Salisbury, W. D. & Pearson, R. A. & Pearson, A. W. & Miller, D. W. (2001). Perceived security and World Wide Web purchase intention. *Industrial Management & Data Systems*, 101, (4), pp. 165–177.

Schierz, P. G. & Schilke, O. & Wirtz, B. W. (2010). Understanding consumer acceptance of mobile payment services: An empirical analysis. *Electronic Commerce Research and Applications*, 9, (3), pp. 209–216. DOI: 10.1016/j.elerap.2009.07.005.

Shin, D.-H. (2010). The Effects of Trust, Security and Privacy in Social Networking: A Security-Based Approach to Understand the Pattern of Adoption. *Interacting with Computers*, 22, (5), pp. 428–438.

Shneiderman, B. (2000). Designing Trust Into Online Experiences. *Communications of the ACM*. 43, (12), pp. 34–40.

Stroborn, K. & Heitmann, A. & Leibold, K. & Frank, G. (2004). Internet payments in Germany: a classificatory framework and empirical evidence. *Journal of Business Research*, 57, (12), pp. 1431–1437.

Suomen virallinen tilasto (SVT): Televiestintä [web publication]. (2008). Helsinki: Tilastokeskus [cited: 2.3.2011]. Available online: http://www.stat.fi/til/tvie/2008/tvie_2008_2009-06-09_tie_001_fi.html.

Tsalgatidou, A. & Pitoura, E. (2001). Business models and transactions in mobile electronic commerce: Requirements and properties. *Computer Networks* 37, 221–236.

Varadharajan, V. (2000). Security enhanced mobile agents. In *Proceedings of 7th ACM conference on computer and communication security*, pp. 200–209. DOI=http://doi.acm.org/10.1145/352600.352632

Venkatesh, V. & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies, *Management Science*, 46, (2), pp. 186–204. ISSN: 0025-1909. DOI: 10.1287/mnsc.46.2.186.11926

Venkatesh, V. & Morris, M. G. & Davis, G. B. & Davis, F. D. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly*, 27, (3), pp. 425–478.

Vijayasarathy, L.R. (2004). Predicting consumer intentions to use online shopping: The case for an augmented technology acceptance model, *Information and Management*, 41, (6), pp. 747–762.

Wang, Y.-S. & Lin, H.-H. & Luarn, P. (2006). Predicting consumer intention to use mobile service. *Information Systems Journal*, 16, (2), pp. 157–179.

Wang, Y.-S. & Wang, Y.-M. & Lin, H.-H. & Tang, T.-I. (2003). Determinants of user acceptance of internet banking: An empirical study, *International Journal of Service Industry Management*, 14, (5), pp. 501–519.

Weiss, S. (2002). *Handheld Usability*, John Wiley & Sons, Hoboken, NJ.

West, R. (2008). The Psychology of Security. *Communications of the ACM*, 51, (4), pp. 34–40. DOI: 10.1145/1330311.1330320

Wright, P. & McCarthy, J. & Meekison, L. (2003). Making Sense of Experience. In Blythe, M. A. & Overbeeke, K. & Monk, A. F. & Wright, P. C. (eds.). *Funology: From Usability to Enjoyment*, pp. 43–54. Kluwer Academic Publishers, Dordrecht. ISBN: 1-4020-1252-7

Wu, J.-H. & Wang, S.-C. (2005). What drives mobile commerce? An empirical evaluation of the revised technology acceptance model, *Information and Management*, 42, (5), pp. 719–729.

Yenisey, M. M. & Ozok, A. A. & Salvendy G. (2005). Perceived security determinants in e-commerce among Turkish university students. *Behaviour & Information Technology*, 24, (4), pp. 259–274.

Zhao-fu, T. & Hao, X. & Ning-ning, X. (2010). Consumers' Perceived Security Risks in E-commerce: A Survey Study. *International Conference on Computer Science and Information Technology (ICCSIT)*, (July), pp. 532–535.

Zucker, L.G. (1986). Production of trust: Institutional sources of economic structure, 1840–1920. *Research in Organizational Behavior*, 8, pp. 53–111.

Appendix A: Questions of the web survey

In Finnish	In English
Opiskelijanumero (HUOM! Tätä tietoa käytetään ainoastaan suorituksen kirjaamiseen, eikä sitä yhdistetä vastauksiisi mitenkään.)	Student number (NB This information will only be used as an indication of a completed course assignment, and it will not be connected to your responses.)
Sukupuoli • Mies • Nainen	Gender • Male • Female
Ikä	Age
Koulutusohjelma • Tik • Inf • Tlt • Muu:	Degree programme • CSE • IN • CE • Other:
Opintojesi vaihe • Kandivaiheen opinnot • Maisterivaiheen opinnot	Phase of studies • Bachelor level studies • Master’s level studies
Omistatko älypuhelimen? • Kyllä • En	Do you own a smart phone? • Yes • No
Oletko ladannut kännykkääsi sovelluksia? • Kyllä • En	Have you installed applications to your mobile phone? • Yes • No
Kuinka usein käytät Internetiä matkapuhelimellasi? • Päivittäin • Muutaman kerran viikossa • Muutaman kerran kuukaudessa • Harvemmin • En koskaan	How often do you use Internet with your mobile phone? • Daily • A few times a week • A dew times a month • Less frequently • Never
Koettu turvallisuuden tunne	**Perceived security in mobile authentication**

mobiilipalvelujen tunnistautumisessa Tässä osiossa selvitetään näkemyksiäsi tunnistautumisen (authentication) turvallisuudesta mobiilipalveluissa. Tunnistautumisella tarkoitetaan tässä kyselyssä sitä, että käyttäjää pyydetään palveluun kirjauduttaessa tai palvelussa toimenpiteitä suoritettaessa syöttämään henkilökohtaisia tunnistautumistietoja (käyttäjätunnus, salasana, verkkopankkitunnus, luottokorttinumero tmv.). Mobiilipalveluilla viitataan mihin tahansa verkkopohjaiseen, tunnistautumistietoja tai muita henkilökohtaisia tietoja vaativaan palveluun (esim. Facebook, sähköpostipalvelu, verkkopankki tai verkkokauppa), jota käytetään matkapuhelimella.	This part of the survey includes questions to determine your perceptions of the authentication security in mobile services. In this survey, authentication means that user is asked to enter certain personal identification information (username, password, Internet banking passcodes, credit card number etc.) when logging in to the service, or while performing certain actions in the service. Mobile service, in turn, is whatever Internet-based service requiring user authentication or other personal information (e.g. Facebook, email service, Internet bank or shop) that is used with a mobile phone.
1. Kuinka paljon käytät tunnistautumista vaativia mobiilipalveluja? • Päivittäin • Muutamaan kerran viikossa • Muutamaan kerran kuukaudessa • Harvemmin • En koskaan	1. How often do you use mobile services that require authentication? • Daily • A few times a week • A dew times a month • Less frequently • Never
2. Kuinka paljon mietit turvallisuusasioita tunnistautuessasi mobiilipalveluihin? (HUOM! Jos vastasit kysymykseen 1 ”en lainkaan”, vastaa kysymyksiin 2-24 siten, että korvaat mobiilipalvelun tietokoneella käytettävällä verkkopalvelulla.) • Paljon • Melko paljon • Melko vähän	2. How much do you think about security issues while authenticating in mobile services? (NB If you responded ”never” to question 1, please answer questions 2-24 in such a way that mobile service is replaced with a regular Internet service that is used with a computer.) • Greatly • Fairly much • Fairly little

• Vähän • En lainkaan	• Little • Not at all
3. Miten turvalliseksi koet palveluun/palvelussa tunnistautumisen matkapuhelimella? • Hyvin turvalliseksi • Melko turvalliseksi • Melko turvattomaksi • Turvattomaksi	3. How secure do you consider mobile authentication to be? • Very secure • Fairly secure • Fairly insecure • Insecure
4. Mitkä tekijät vaikuttavat valitsemaasi mielipiteeseesi?	4. What factors affect the opinion you expressed?
5. Minkälaisten palveluiden yhteydessä turvallisuus on mielestäsi erityisen tärkeää? Entä millaisten palveluiden tapauksessa olet vähemmän huolissasi turvallisuusasioista?	5. Are there any types of services where security is particularly important? How about services that make you less concerned about security?
6. Vaikuttaako kokemuksesi määrä mobiilipalveluista kokemaasi turvallisuuteen tunnistautumisessa? Miten?	6. Do you think that your prior experience of mobile services affects your judgment of the perceived security? How?
7. Kuinka tietoinen olet mobiilipalveluissa käytössä olevista tietoturvaominaisuuksista? • Hyvin tietoinen • Melko tietoinen • Melko vähän tietoinen • Vähän tietoinen • En lainkaan tietoinen	7. How aware are you of the security mechanisms that are utilized in the mobile services? • Well aware • Fairly aware • Fairly little aware • Little aware • Unaware
8. Miten ne näkyvät sinulle palveluja käyttäessäsi?	8. How are these mechanisms visible while you use the services?
9. Kuinka paljon havaitsemasi tietoturvaominaisuudet palvelussa vaikuttavat kokemaasi turvallisuuden tunteeseen? • Paljon • Melko paljon • Melko vähän	9. How much do observed security mechanisms in the services affect your judgement of the perceived security? • Greatly • Fairly much • Fairly little

• Vähän • En lainkaan	• Little • Not at all
10. Kumman tavan koet turvallisemmaksi: tietokoneella tapahtuvan tunnistautumisen vai matkapuhelimella tapahtuvan tunnistautumisen? • Tietokoneella tapahtuvan • Matkapuhelimella tapahtuvan • En näe eroja mainittujen tapojen välillä	10. Which one do you consider as more secure alternative: authentication with a computer or with a mobile phone? • Computer • Mobile phone • Do not see difference between the two
11. Mikäli edellä mainituilla tilanteilla on mielestäsi eroa, niin mitä nämä erot ovat ja vaikuttavatko ne päätökseesi käyttää mobiilipalveluja?	11. If you thought that there was a difference between the two alternatives, then what was the difference and does it affect your decision to use or not use mobile services?
12. Onko palveluja, joita et käytä/käyttäisi matkapuhelimellasi turvallisuuteen liittyvistä syistä? Mitä nämä palvelut ovat?	12. Are there any services that you do not/ would not use with your mobile phone because of security concerns? What are these services?
13. Vaikuttaako käyttöympäristö kokemaasi turvallisuuden tunteeseen mobiilitunnistautumisessa? Miten?	13. Does use context affect your judgement of perceived security in mobile authentication? How?
14. Vaikuttaako kokemaasi turvallisuuden tunteeseen se, tarjoaako tunnistautumisen käyttämäsi mobiilipalvelun tarjoava yritys itse vai toteutetaanko tunnistautuminen jonkin ulkopuolisen toimijan toimesta? • Kyllä • Ei	14. Does your judgement of perceived security differ depending whether authentication is provided by the service provider itself or by a third-party company? • Yes • No
15. Mitkä toimijat koet turvallisiksi? Mistä syistä?	15. What service providers do you consider as trustworthy? Why?
16. Onko kokemuksesi ulkopuolisen toimijan tarjoaman tunnistautumisen turvallisuudesta sama riippumatta siitä, missä palvelussa sitä käytetään?	16. Is your judgement regarding perceived security of third-party authentication same regardless of the service where it is utilized? • Yes

• Kyllä • Ei	• No
17. Kuinka paljon tunnistautumisen tarjoavan yrityksen brändin tunnettuus/maine vaikuttaa kokemaasi turvallisuuden tunteeseen? • Paljon • Melko paljon • Melko vähän • Vähän • Ei lainkaan	17. How much does brand/reputation of the authentication provider affect your judgement of perceived security? • Greatly • Fairly much • Fairly little • Little • Not at all
18. Miten palvelun visuaalinen ilme vaikuttaa kokemaasi turvallisuuden tunteeseen tunnistauduttaessa? Mitkä asiat lisäävät ja mitkä vähentävät turvallisuuden tunnetta?	18. How does the visual appearance of the service affect your judgement of perceived authentication security? What factors increase and what factors decrease the feeling of security?
19. Kuinka paljon aikaisemmat hyvät/huonot kokemuksesi mobiilipalveluista vaikuttavat kokemaasi turvallisuuden tunteeseen ottaessasi uuden palvelun käyttöön? • Paljon • Melko paljon • Melko vähän • Vähän • Ei lainkaan	19. How much do prior good/bad experiences of mobile services affect your judgement of perceived security when you start using a new service? • Greatly • Fairly much • Fairly little • Little • Not at all
20. Millä tavalla hyvät/huonot kokemukset yhdestä mobiilipalvelusta vaikuttavat muihin palveluihin suhtautumiseen?	20. How do good/bad experiences of one mobile service affect your attitude towards other services?
21. Kuinka paljon tuttujen ja kavereiden kokemukset/suositukset vaikuttavat kokemaasi turvallisuuteen mobiilipalvelujen tunnistautumisessa? • Paljon • Melko paljon • Melko vähän	21. How much do experiences/ recommendations of friends and acquaintances affect your judgement of perceived security in mobile authentication? • Greatly • Fairly much • Fairly little

• Vähän • Ei lainkaan	• Little • Not at all
22. Miten suhtaudut lähtökohtaisesti uusiin mobiilipalveluihin? • Hyvin luottavaisesti • Melko luottavaisesti • Melko varauksella • Hyvin varauksella	22. What is your attitude towards new mobile services? • Very trusting • Fairly trusting • Fairly suspicious • Very suspicious
23. Onko yleinen suhtautumisesi mobiilipalvelujen tunnistautumisen turvallisuuteen muuttunut? • Suhtautumiseni on muuttunut huomattavasti positiiviseen suuntaan • Suhtautumiseni on muuttunut hieman positiiviseen suuntaan • Suhtautumiseni ei ole muuttunut • Suhtautumiseni on muuttunut hieman negatiiviseen suuntaan • Suhtautumiseni on muuttunut huomattavasti negatiiviseen suuntaan	23. Has your general attitude regarding security of mobile authentication changed? • Attitude has changed considerably for the better • Attitude has changed slightly for the better • Attitude has not changed • Attitude has changed slightly for the worse • Attitude has changed considerably for the worse
24. Mitkä tekijät lisäisivät turvallisuuden tunnettasi matkapuhelimella tapahtuvassa tunnistautumisessa?	24. What factors would improve your judgement of perceived mobile authentication security?
25. Jos matkapuhelimessasi olisi sisäänrakennettuna turvaelementti, jota käyttäen voisit tunnistautua tietyissä palveluissa, niin olisitko valmis käyttämään kyseistä ominaisuutta? Näetkö palvelukohtaisia eroja sen suhteen, missä olisit valmis käyttämään toimintoa? (Tunnistautumistietosi olisivat siis tallennettuna turvaelementtiin ja niitä käytettäisiin asioitaessa yhteensopivissa	25. If your mobile phone had a built-in security element that you could utilize in authenticating to certain services, would you be willing to use this feature? Would you be willing to use the feature in all services or just certain services? (In the highlighted solution, your authentication data would be stored inside the security element and they would be used while using the compatible services.)

palveluissa.)	
26. Olisitko valmis vaihtamaan matkapuhelinta saadaksesi edellä mainitun toiminnallisuuden käyttöösi?	26. Would you be ready to change your mobile phone in order to be able to use the highlighted feature?