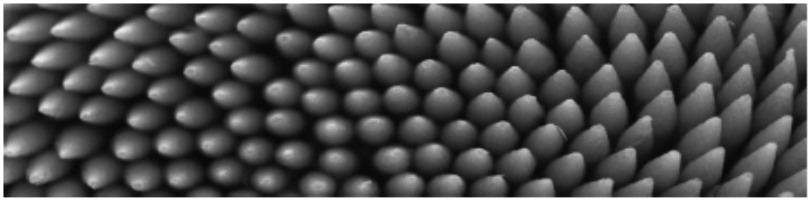
Helsinki University of Technology
Publications in Telecommunications Software and Multimedia
Teknillisen korkeakoulun tietoliikenneohjelmistojen ja multimedian julkaisuja
Espoo 2007 TML-A19

BRIDGING THE GAP BETWEEN HUMAN AND MACHINE TRUST

Applying methods of user-centred design and usability to computer security

Kristiina Karvonen



TEKNILLINEN KORKEAKOULU
TEKNISKA HÖGSKOLAN
HELSINKI UNIVERSITY OF TECHNOLOGY
TECHNISCHE UNIVERSITÄT HELSINKI
UNIVERSITE DE TECHNOLOGIE D'HELSINKI

Helsinki University of Technology
Publications in Telecommunications Software and Multimedia
Teknillisen korkeakoulun tietoliikenneohjelmistojen ja multimedian julkaisuja
Espoo 2007 TML-A19

BRIDGING THE GAP BETWEEN HUMAN AND MACHINE TRUST

Applying methods of user-centred design and usability to computer security

Kristiina Karvonen

Dissertation for the degree of Doctor of Science in Technology to be presented with due permission of the Department of Computer Science and Engineering, for public examination and debate in Auditorium T2 Helsinki University of Technology (Espoo, Finland) on May 25, 2007 at 12 noon.

Helsinki University of Technology
Department of Computer Science and Engineering
Telecommunications Software and Multimedia Laboratory

Teknillinen korkeakoulu
Tietotekniikan osasto
Tietoliikenneohjelmistojen ja multimedian laboratorio

Helsinki University of Technology
Telecommunications Software and Multimedia Laboratory
P.O.Box 5400
FIN-02015 TKK
Tel. +358 9 4511
Fax +358 9 465 077

http://www.tml.tkk.fi

ISBN 978-951-22-8785-7 (printed version)
ISSN 1456-7911
ISBN 978-951-22-8786-4 (electronic version)
ISSN 1455-9722

Cover illustration

Multiprint Oy/Otamedia
Espoo, Finland 2007

ABSTRACT OF DOCTORAL DISSERTATION	HELSINKI UNIVERSITY OF TECHNOLOGY P.O. BOX 1000, FI-02015 TKK http://www.tkk.fi

Author Kristiina Karvonen

Name of the dissertation
Bridging the Gap between Human and Machine Trust

Manuscript submitted 11.6.2006	Manuscript revised 10.4.2007
Date of the defence 25.5.2007	
☐ Monograph	☒ Article dissertation (summary + original articles)

Department	Computer Science
Laboratory	Telecommunications Software and Multimedia
Field of research	Telecommunications
Opponent(s)	Professor L. Jean Camp
Supervisor	Professori Antti Ylä-Jääski
Instructor	Professori Antti Ylä-Jääski

Abstract

This work presents methods for improving the usability of security. The work focuses on trust as part of computer security. Methods of usability and user-centred design present an essential starting point for the research. The work uses the methods these fields provide to investigate differences between machine and human trust, as well as how the technical expressions of trust could be made more usable by applying these methods. The thesis is based on nine publications, which present various possibilities to research trust with user-centric methods. The publications proceed chronologically and logically from the first user interviews about trust, trusting attitudes and behaviours in general to the actual design and usability testing of user interfaces for security applications, finally presenting the outcomes and conclusions of the research.

The work also presents a review of relevant previous work in the area, concentrating on work done in the fields of usability and user-centred design. The work is of cross-disciplinary nature, falling into the areas of human-computer interaction, computer science and telecommunications. The ultimate goal of the conducted research has been to find out 1) how trust is to be understood in this context; 2) what methods can be used to gain insight into trust thus defined; and, finally, 3) what means can be used to create trust in the end users in online situations, where trust is needed. The work aims at providing insight into how trust can be studied with the methods provided by user-centred design and usability. Further, it investigates how to take understanding of trust formation in humans into account when attempting to design trust-inducing systems and applications.

The work includes an analysis and comparison of the methods used: what kinds of methods to study trust exist in the field of usability and user-centred design. Further, it is evaluated, what kind of results and when can be reached with the different methods available, by applying a variety of these methods. Recommendations for the appropriate application of these methods when studying the various parts of trust is one of the outcomes. The results received with the methods used have also been compared with results received by others by applying alternative methods to the same research questions.
On a conceptual level, the work contains an analysis of the concept of trust. It also contains a brief investigation into both technical and humane ways to express trust, with a comparison between the two.

Keywords Trust, trust management, computer networks, usability, user-centred design, computer security

ISBN (printed)	978-951-22-8785-7	ISSN (printed)	1456-7911
ISBN (pdf)	978-951-22-8786-4	ISSN (pdf)	1455-9722
Language	English	Number of pages	88 + 76
Publisher	Helsinki University of Technology, Otamedia Oy		

Print distribution

☒ The dissertation can be read at http://lib.tkk.fi/Diss/

VÄITÖSKIRJAN TIIVISTELMÄ	TEKNILLINEN KORKEAKOULU PL 1000, 02015 TKK http://www.tkk.fi

Tekijä Kristiina Karvonen

Väitöskirjan nimi
Bridging the Gap between Human and Machine Trust

Käsikirjoituksen päivämäärä 11.6.2006	Korjatun käsikirjoituksen päivämäärä 10.4.2007
Väitöstilaisuuden ajankohta 25.5.2007	
☐ Monografia	☒ Yhdistelmäväitöskirja (yhteenveto + erillisartikkelit)

Osasto	Tietotekniikan osasto
Laboratorio	Tietoliikenneohjelmistojen ja multimedian laboratorio
Tutkimusala	Tietoliikenneohjelmistot
Vastaväittäjä(t)	Professor L. Jean Camp
Työn valvoja	Professori Antti Ylä-Jääski
Työn ohjaaja	Professori Antti Ylä-Jääski

Tiivistelmä
Tässä työssä esitellään menetelmiä tietoturvamekanismien käytettävyyden parantamiseen. Työ keskittyy tarkastelemaan erityisesti luottamusta tietoturvan osana. Keskeisenä lähtökohtana ovat käytettävyyden ja käyttäjäkeskeisen suunnittelun menetelmät. Työssä kartoitetaan näiden menetelmien kautta eroja teknisen ja inhimillisen luottamuksen ilmaisutapojen ja ehtojen välillä, sekä miten luottamuksen teknisiä ilmaisutapoja voitaisiin tehdä käyttäjäystävällisemmiksi näitä menetelmiä soveltamalla. Työ pohjaa yhdeksään julkaisuun, joissa on esitetty erilaisia mahdollisuuksia lähestyä luottamuksen käsitettä käyttäjäkeskeisen suunnittelun menetelmin. Julkaisut etenevät loogisesti ja kronologisesti ensimmäisistä, luottamusta yleisesti kartoittavista käyttäjähaastatteluista varsinaisten tietoturvakäyttöliittymien suunnitteluun ja käytettävyystesteihin, sekä lopulta saatujen johtopäätösten ja tulosten käsittelyyn.

Työ esittelee myös tämän tutkimuksen kannalta keskeiset käyttäjäkeskeisin menetelmin aiemmin tehdyt tutkimukset tuloksineen. Työ kuuluu tietoturvan, tietoliikenteen ja käytettävyystutkimuksen alaan ja on luonteeltaan monitieteinen. Työn pohjimmaisena tavoitteena on ollut selvittää 1) mitä luottamus tässä yhteydessä on; 2) millaisin menetelmin luottamuksesta voidaan saada tietoa; sekä 3) millaisin keinoin voidaan herättää loppukäyttäjissä luottamusta sellaisissa verkonkäyttötilanteissa, joissa luottamusta tarvitaan.

Edellä esitetyn lisäksi työ sisältää menetelmäanalyysin ja -vertailun: millaisia menetelmiä on olemassa luottamuksen tarkasteluun käytettävyyden ja käyttäjäkeskeisen suunnittelun näkökulmasta. Lisäksi arvioidaan, miten ja millaisia tuloksia voidaan saada eri menetelmiä käyttäen. Metodologisesti työn sisältönä on ollut testata, miten ja milloin erilaiset käytettävyys- ja käyttäjäkeskeisen suunnittelun menetelmät soveltuvat luottamuksen alueen tutkimiseen. Tämä testaus on suoritettu erilaisia menetelmiä kokeillen ja tulokset raportoiden. Työn osatuloksena on siten suositus näiden menetelmien käytöstä luottamuksen eri osa-alueiden tutkimuksessa. Saatuja tuloksia on verrattu tuloksiin, joita on saatu tutkimalla samaa aihetta vaihtoehtoisin menetelmin.
Käsitteellisellä tasolla työn sisältöön kuuluu luottamuksen käsitteen analysointi, luottamuksen teknisten ilmaisujen tarkastelu, sekä käyttäjien ilmaiseman luottamuksen tarkastelu ja edellisten keskinäinen vertailu. Työn tuloksena on myös lista luottamustutkimukselle oleellisista jatkotutkimusalueista ja -aiheista.

Asiasanat Luottamus, luottamuksenhallinta, tietoverkot, käytettävyys, käyttäjätutkimus, tietoturva

ISBN (painettu)	978-951-22-8785-7	ISSN (painettu)	1456-7911
ISBN (pdf)	978-951-22-8786-4	ISSN (pdf)	1455-9722
Kieli	Englanti	Sivumäärä	88 + 76
Julkaisija	Helsinki University of Technology, Otamedia Oy		

Painetun väitöskirjan jakelu

☒ Luettavissa verkossa osoitteessa http://lib.tkk.fi/Diss/

To the memory of my mother
Annikki Karvonen (1943-2002)

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

I am grateful to have been able to work with such an intriguing theme as trust as part of usability of security, essentially, is. However, this is not an accomplishment I can completely claim my own, but it is to a great extent that I am in gratitude towards my co-authors and colleagues in Telecommunications Software and Multimedia Lab at the Helsinki University of Technology. My warm thanks go to the whole TeSSA project team I was a member of when starting my research. I would especially like to thank Markku Laukka, a great colleague, and Dr. Tuomas Aura, Dr. Arto Karila, and Professor Hannu H. Kari and Professor Petri Vuorimaa for their support on the way. I would also like to thank all my current colleagues in the Trustinet project, for their support on and interest in my work. I would also like to thank my supervisor, Professor Antti Ylä-Jääski, for his help during the procedure. A big thank you also goes to Professors N. Asokan and Kaisa Nyberg, and to Jaakko Lehtinen, and Miika Komu, for being such good colleagues, and to Laura Takkinen, Sanna Suoranta as well as Eeva Kykkänen and the staff at Computer Science building, especially Juho Komu and Raimo Ruottinen, for all their help and support. Many thanks also to all my friends, and to Tiina Alanko and Ronan MacLaverty, who was kind enough to proofread the manuscript and give useful comments as he went along. Therefore, he is to be thanked for the English where it is good, whereas I am to be acknowledged for the parts of lesser linguistic quality.

I was very lucky in the selection of my pre-examiners Professor Sirkka Jarvenpaa and Professor M. Angela Sasse, who represent the utmost top in their respective fields. Their feedback has been invaluable and I am greatly indebted to them for their suggestions in making this thesis a better one. I am happy to thank with deep gratitude my opponent Professor L. Jean Camp for taking the time from her busy schedule to read the manuscript and for examining and debating my views.

This research would not have been possible without the financing from the industrial partners and TEKES, the National Technology Agency of Finland. Without the participating individuals in my user studies in Finland, Sweden, and Iceland, this work would have been not only impossible but also meaningless – I wish to thank them all. Special thanks go to my co-authors Lucas Cardholm, Stefan Karlsson, Ursula Holmström, Dr. Pekka Nikander, and to Jarmo Parkkinen, a dear friend and always fun to work with. A big thank you also to Professor Marta Kristin Larusdottir from Reykjavík University for an insightful talk as well as for helping me with my user studies in Iceland. Warmest thanks also go to Ingimar Fridriksson and the other personnel of Reykjavík University for the practical arrangements of my user studies in Reykjavík. I would also like to thank Professors Mauri Kaipainen, Jukka Vanhala, Dianne Cyr, Noam Tractinsky, and Jens Riegelsberger for their collegial support.

I would like to thank my father Pekka Karvonen, for the love and the substantial financial support, without which it would have been difficult to pursue my university studies. Thanks also go to my sister Jaana Valo for always being there for me. My dear cat friend Ingel means the world to me and will probably be pleased once she realises that this overture turned into an undertaking has finally reached its end and we have time for the important things in life, such as play, much more than before. Finally, I want to thank Simo for the aesthetics he has brought into my life, as well as to the cover of this book.

I dedicate this work to the memory of my dear mother, who passed away unexpectedly whilst I was in the midst of trying to finalise this work for the first time, and whom I miss more than any simple expression may ever communicate.

Helsinki, May 2, 2007
Kristiina Karvonen

LIST OF PUBLICATIONS

This thesis is based on the following publications:

[P1] Karvonen, K. (1999). Creating Trust, Proceedings of the Fourth Nordic Workshop on Secure IT Systems (NordSec'99), November 1-2, 1999, Kista, Sweden, pp. 21-36

[P2] Karvonen, K. (1999). Enhancing Trust Online, Proceedings of PhDIT'99: Ethics in Information Technology Design. Second International Workshop on Philosophy of Design and Information Technology, 16-17 December, 1999, Saint-Ferréol, Toulouse, France, pp. 57-64

[P3] Nikander, P., Karvonen, K. (2001). Users and Trust in Cyberspace, in B. Christianson, B. Crispo, J.A. Malcolm, M. Roe (Eds.): Security Protocols, 8th International Workshops Cambridge, UK, April 3-5, 2000, Revised Papers LNCS 2133, Springer-Verlag Berlin Heidelberg 2001, pp. 24-35

[P4] Karvonen, K., Cardholm, L., Karlsson, S. (2000). Cultures of Trust: A Cross-Cultural Study on the Formation of Trust in an Electronic Environment, in Proceedings of the Fifth Nordic Workshop on Secure IT Systems, NordSec 2000, 12-13 October, 2000, Reykjavik, Iceland , pp. 89-100

[P5] Karvonen, K, Holmström, U. (2000). Expressing Trust, in Proceedings of NordiCHI 2000 (short papers), The First Nordic Conference on Computer-Human Interaction, 23-25 October 2000, Royal Institute of Technology, Stockholm, Sweden, CD proceedings, ed. Gulliksen, J et al, 2pp.

[P6] Karvonen, K. (2000). Experimenting with Metaphors for All: A User Interface for a Mobile Electronic Payment Device, in Proceedings of 6th ERCIM Workshop "User Interfaces for All" (UI 4 All), 25-26 October, 2000, Convitto della Calza, Florence, Italy, pp. 183-188

[P7] Karvonen, K (2000). The Beauty of Simplicity, in Proceedings of the ACM Conference on Universal Usability (CUU 2000), November 16-17, 2000, Washington DC, USA, pp. 85-90

[P8] Karvonen, K. (2001). Designing Trust for a Universal Audience: A Multicultural Study on the Formation of Trust in the Internet in the Nordic Countries (invited paper), in the Proceedings of the First International Conference on Universal Access in HCI (UAHCI'2001), August 5-10, 2001, New Orleans, LA, USA, pp. 1078-1082

[P9] Karvonen, K., Parkkinen, J. (2001). Signs of Trust, in the Proceedings of the 9th International Conference on HCI (HCII2001), August 5-10, 2001, New Orleans, LA, USA, pp. 1076-1080

LIST OF ABBREVIATIONS

CA	Certificate Authority
CHI	Computer-Human Interaction, see also HCI
EPIC	Electronic Privacy Information Center
HCI	Human-Computer Interaction, see also CHI
IP	Internet Protocol
IPsec	Internet Protocol Security
P2P	Peer-to-Peer
PDA	Personal Digital Assistant
PKI	Public Key Infrastructure
SA	Security Association
TCB	Trusted Computing Base
TCP/IP	Transmission Control Protocol/Internet Protocol
TN	Trust Negotiation
TTP	Trusted Third Party
UCD	User-Centred Design
UE	User Experience, see also UX
UI	User Interface
UX	User Experience, see also UE

1 Introduction

> *"Securing the interaction between people and just about anything is a big problem. People don't understand computers. Computers are magical boxes that do things. People believe what computers tell them. People just want to get their jobs done. People don't understand risks. They may, in a general sense, when the risk is immediate. People lock their doors and latch their windows. They check that no-one is following them when they walk down a darkened alley. People don't understand subtle threats. They don't think that a package could be a bomb, or that the nice convenience store clerk might be selling credit card numbers to the mob on the side. And why should they? It almost never happens."*
>
> - Bruce Shneier (2000)

At the turn of the millennium, lack of trust was considered one of the major obstacles to developing successful ecommerce enterprises (e.g., Ecommerce Trust Study 1999, Jarvenpaa and Tractinsky 1999, [P1], Nielsen 1999a). It was realised that in order for the ecommerce to flourish and any online service to be successful, creating trust would become means to an end – a necessity. Furthermore, it was realised that understanding the *real-world trust* would be crucial to understanding the actual security of any transactions online — maybe even more so than creating the technological solutions for these transactions (e.g. Friedman 2000, Salam et al 2003). Trust is one of the essential ingredients of the usability of security – a usability demand that is novel compared to "ordinary" usability measures. Trust forms the basis for all online transactions (Friedman 2000), and a trusting attitude towards computers in general may help put the user at ease when operating often complex systems – a description well suited to computer security applications. Trust is needed for using appliances that are critical security-wise. To enhance it, we need to understand what *trust* in general is made of – how users perceive it, and how this relates to the trust expressed by machines.

Current computer security technologies are complicated and were developed with the technologically advanced in mind. As use situations have grown more complex and risky, however, there has emerged a new need for the managing of security – and trust – to become more understandable all users. More and more "ordinary" people, without any former experience with security issues or technologies will have to learn to manage these security features now, when microchips can be everywhere, our environments and homes are flooded with ubiquitous technology, and the mobile technology is always with us in our pockets – wherever we go. User involvement is now often necessary, which has had the effect that trust issues are becoming more and more pending and explicit. This is happening also in the area of ecommerce and the online transactions it brings with it. No one will want to give away his or her credit card number to anyone, if there is no trust. The same applies for other types of private information, such as social security numbers or medical health data, for example. Yet, people would like to be able to fully utilise these new types of services and media for all types of transactions, also those requiring a high level of trust.

Users are often considered to be the weakest link in the security of online transactions (Adams and Sasse 1999b), and rightly so, for what else could they be, when they are not provided with sufficient amount of information and support on making informed decisions in online situations. Users cannot be expected to be able to make rational choices of whether an operation is secure and trustworthy or not, if they are not given the information to base their decisions on. The demand for easy-to-use, easy-to-understand information is paramount for creating usable security. This requirement is well expressed in the following quote by Eric Ketelaar, in his demand for trustworthy information (Ketelaar 1997):

> *"Why do we demand more of the quality of food or a car than we demand of that other essential: information? Reliability and authenticity determine the credibility and the usefulness of information. These concepts, developed in different cultures and at different times, are essential for our information society in its dependence on trust in information. In the creation and distribution of digital information, conditions should be met to ensure the reliability and authenticity of the information."*

Why indeed would we demand less from information, than we demand in other areas in our daily lives, in order to trust? Yet both the information and the means to deal with that information are often lacking, when a user encounters in interactions with computer security. Still today, there exists a huge gap between what users should know and what they do know about how computer security works. Users do, however, repeatedly report a craving for more understandable security information, in order to be able to make better decisions on online behaviours and access, and be better able to protect their children as well (Safer Internet 2006).

Until today, the technical representations of trust have not really had anything to do with trust as it is known in the world of users. The formal representations of trust have been based more on the formal models used than the real user requirements posed by the actual users [P3]. This has created a gap between the technical ways to express trust and in the way real people tend to express trust and to understand trust expressions of others. In order to increase usability of controlling trust, the technical representations will have to come closer and take into account the real-world users of the systems behind these representations. A lot of work has been done in fields of analysing and modelling trust in the technical sense and in providing infrastructures for expressing trust and authorisation in open systems in a machine-to-machine interaction (see e.g. [P3] for a number of references). However, due to more complicated use situations, this needs to be accomplished in the human-machine interaction also, in a way that is understandable to both the machine and the user. The users need to be able to handle security features of a given system in a novel way: to be able to *manage*, *express* and *control* trust. Furthermore, all this needs to be accomplished in a way that is *understandable* to the common man, not just to the technically advanced and knowledgeable user. Users have been reluctant to trust the services they cannot really fathom, and same goes for the concepts behind the initial countermeasures against this distrust, such as Trusted Third Parties (TTP) and Certificate Authorities (CA) that still remain unfamiliar to most online users. In effect, the sources of information for whether to trust or not cannot be these strange bodies of the virtual world, but the more familiar ones: the recommendations given by friends, colleagues, and family members; the daily news; even rumours and hearsay. As their first choice, people would trust other people, not machines, regardless of the media.

If these gaps between what users know and understand and what they are provided with are not closed in a proper manner, we are facing two kinds of security risks [P5]:

1. The users will not be able to handle trust issues in the right way, and will continue creating a security risk. Users will definitely be the "weakest link" in the chain of security in that case.
2. Without getting to know the real users and the world they live in, as well as what "trust" means for the common person, we are not able to answer the security needs of users as fully as we can, if we know for whom we are designing.

Through gathering knowledge about the real-world use situations with the methods provided by User-Centred Design (UCD), we will be likely to be able to create better and more easy-to-use security services the properties and functionalities of which will be used to full extent, empowering the users. This means that in order to create the kind of services that will meet all these requirements, we will have to find out

- How users experience trust, what they consider relevant to the issues of trust, and in what kind of use situations trust is needed, and what this trust is made of, as well as
- What kind of answers might we have for these needs in the technical world, or what kind of solutions would be likely to be most successful and relevant for the users.

While gaining the trust of online users may be slow and painstaking from the entrepreneur's point of view, losing trust happens quickly. A single violation of trust may destroy the achievements of trust over a period of months or even years (Nielsen 1999a, Ecommerce Trust Study 1999, Cardholm 1999). Also, in an open network like the Internet you cannot trust everyone to be playing by the rules. Obviously, there is a need for some security mechanism to prevent others from doing harmful things in risky situations – either by mistake or on purpose. With technologies such as mobile code, software agents and distributed computing, there is a need to express, in a way understandable for the machines, who is allowed to do what and under what conditions – who is trusted and who is not. With the number of parties involved, it is impractical to base these decisions on traditional access control lists. Instead, these decisions should be based on the kind of recommendations and expressions of trust by other parties that are computational somehow [P3].

On basis of the work at hand, it is no surprise that we have witnessed the upsurge of such recommendation-based systems. In these, peers can build up the reputation of them and of each other by both being tracked for their activities, as well as by providing explicit statements of their actions and preferences, usually tied to the usage of a particular service, such as eBay (www.ebay.com) or Amazon (www.amazon.com), for example. Further, they can usually do this in their own language, in familiar terms and using real life expressions. However, even if such embedding of existing social networks into the online environment has proved successful, there remains a plethora of unanswered questions in the usage of these systems to promote trust as well.

One such problem is that the trust is not truly *transferable*: the trust recommendations and reputation built in one system is usually accessible for that system alone. To start with, it will be difficult to integrate the various systems a singular user is interacting with one another technically. Also choosing what information to share between which systems is a difficult and represents possibly a risky choice from a user's perspective that may have notable repercussions on the privacy of that user. To give a simple example, currently many users have multiple online identities, which may be only partly overlapping and only loosely connected with each other, if at all. Exchanging information between such identities by accident might greatly damage the user's privacy – for good (Donath and Boyd 2004). The classical study by Good and Krekelberg (2003) already showed how easy it is for the user to make such mistakes – and never become aware of them. A further problem with recommendation-based systems is to decide how to rate the recommendations and how to find the best ones. A lot of work is ongoing in this area. For example (Friedman et al 2004), (Bonhard 2005, Bonhard et al 2005, 2006), (Riegelsberger et al 2006) and (Camp 2006) provide some examples of enriching the recommendations by finding ways to bring in more of the right type of information needed for better accuracy.

Users may also base their trust on false assumptions and false impressions online or offline, and are not always behaving like model citizens, or even with their own best interest in mind. Users cannot really be trusted to flawlessly implement computer security policies, just as they cannot be trusted always to lock their car door or never to lose their keys. All users make mistakes sometimes; they cannot be trusted to do things precisely. People also misunderstand, forget things, are ashamed sometimes to admit they do not know something, and so on. People do not always behave in a rational way – they are also emotional and in real-life as well decide to trust fortune-tellers and suspicious-looking sales clerks. Malicious insiders are often implicitly trusted, as well, which opens up the opportunity for treachery. But that's how humans are – trusting in the wrong situations and on wrong grounds; and benevolent actors

can lead to trust broken, and lost - even when they mean well and act with all the good intentions. In the same way, they cannot be trusted to make intelligent decisions about computer security – at least not all the time.

People should also be distrustful at times. In his book *The Art of Deception*, Kevin Mitnick, a former hacker tells how easy it was to compromise computer security by using so-called "social engineering": manipulating humans (Mitnick et al 2002). In practice, it means, for example, pretending to be someone else, someone trusted or someone with certain rights and to persuade the other person to do what they want, like give out confidential information such as a password, to be misused. A typical example of a social engineering attack is to use email attachments that contain malicious contents that might trigger the victim's machine to start sending loads of spam for example,

Such earlier attacks have led the software vendors to disable automatic execution of attachments. Now, users have to explicitly open and execute attachments for the attack to occur. This presents small hindrance, for in practice many users will do exactly this: open any attachments they receive without questions, thus allowing the attack to work as planned. Perhaps one of the simplest, but still a very effective social engineering trick is to lead a user into thinking that the attacker is an administrator and then request for a password for some purpose. Since this tends to work, users of Internet systems frequently receive messages that contain such a request for a password or credit card information, claiming to be in their best interest: to set up their account, or some other benign operation. These are so-called *phishing* attacks – the confidential information is fished out of the unsuspecting victim. In reality, administrators of computer systems rarely, if ever, need to know the user's password to perform administrative tasks – but this is something most users are unaware of. Work to fight against phishing is flourishing (e.g. Franco 2005, Hartman 2006, Dhamija et al 2006, Cranor et al 2007).

Social engineering is quite effective, and people fall for it repeatedly – and not only people who are naïve in computer security, but the more knowledgeable ones, too. Mitnick, as a former hacker, is the right spokesperson in this matter: after all, via his former actions, he has proved that it is easy to fool humans to tell their passwords or risk the security in some other ways. The reason is they do not understand the risks, what is secure and what is not, and thus users cannot recognise a malicious attack – in any form it may take. Also, no matter how we define what we mean by security, at the core of the issue lies another problem: there may be a great difference between *actual* and *perceived* security. What this means is that the users' ideas about what is secure and what is not might not have anything to do with the actual level of security of, say, a service on the Web (Shneier 2000). When seeking for enhancements to improve the usability of security, it is not enough to make things more user-friendly and easier to understand. We also need to prevent social engineering from taking place: minimise the possibilities for such human fallacies from ever occurring. Only when we reach this stage can we claim the level of usability of security to have truly risen to an acceptable level, and only then can we expect a significant rise for trust the users are ready to express towards online services.

1.1 The scope of this work

This work presents various ways to enhance the usability of security systems. The main focus of the work is on trust within the framework of usability and UCD. These problems and issues are approached mainly from the users' point of view: how real people in real world trust, and how this knowledge might be applied to technical ways to express trust. Thus, the aim of this work is to broaden the view from a protocol-centric approach of online authentication towards considering the actual users, and to provide some initial requirements for future operating

systems and user interface design. A further goal is to find a better understanding of the makings of trust in online environments, and how they might be studied further within the paradigm of user-centred research.

Trust research as part of usability of security is, essentially, a part of the discipline of usability, which falls under the field of Human-Computer Interaction (HCI), sometimes also called Computer-Human Interaction (CHI): studying trust from a user's point of view means studying human behaviour and actions, perceptions, and feelings in relation to trust. HCI is usually defined as study of humans as users of computers (and other respective systems, devices, gadgets, applications and appliances, e.g. mobile phones, TV sets, cars, iPods, diving instruments or what have you); or vice versa, the study of how to make computers more usable via understanding their users. The latter can also be seen as the area of usability (engineering), where the object of study is to engineer the human needs or, in other words, the user requirements, into system design, preferably early on, to ensure better user experience of the product. This goal is thought in general to be reachable via bringing the system model as close as possible to the expected users' mental model of the system (c.f. e.g. Norman 1986, Nielsen 1993 for classical treatises on this area). What this means in practice is that the goal is to create a match between the cognitive capabilities (expectancies, activities) of the user and the system behaviour.

Usability can also be described as a subfield of "User Experience", often abridged as UE or UX. UX is a recent trend, starting somewhere around the turn of the millennium, when classical usability was seen as too narrow in scope, and more emphasis was put into the areas of non-cognitive, affective factors (e.g. Norman 2004, Blythe et al 2003, Jordan 2000, Bødker et al 2003, Egger 2001). However, the terms HCI, usability, and UX are in practice often used interchangeably. This is not too problematic, since the goal is the same, with slightly different emphasis: to study and understand the human as user of some system, device, or application, and the interoperability of the two (e.g. Norman 2004, Saariluoma 2004). In this thesis, the terms usability or HCI are mainly used when referring to the study of humans in context of machines. The usage of two terms is to be understood in the following way: *Usability* is used when referring to the system features and how they are experienced, thus encompassing both Usability and UX. *HCI* is used as an umbrella term to cover the widest possible area of UCD, including usability and UX, and all other approaches and work done to bridge the gap between man and machine in the field of computer science.

As trust is also part of usability of security, we need to have a closer look at this subfield and what it enfolds. Usability of security, or *usable security*, as it is often also called nowadays, can be divided into areas that have been dealt with within this area of study as more or less unconnected patches (e.g. as in Cranor & Garfinkel 2005). These include:

1. User interfaces for managing computer security; their design and usability testing;
2. Problems of authenticating from a user point-of-view, especially usability issues related to passwords;
3. Trustworthiness and trust issues of ecommerce and other online transactions;
4. Privacy issues

From these, this thesis is concentrating mainly only on the study of trust, and other lines of research inside usability of security fall outside the scope of the study for the most part and are dealt with only in relation to dealing with trust issues, as necessary. The excluded areas include usability of authentication (e.g. Basu & Muylle 2003, Ferscha et al 2005), usability of passwords (e.g. Brostoff & Sasse 2003), technical development of trust management (e.g. Nielsen & Krukow 2003; Weippl and Essmayr 2003, Anderson 2003), as well as privacy (e.g. Adams & Sasse 2001, Camp 2003).

Further, the differences between technical and human ways to express trust are explored, and how the two might be combined. The work is multi-disciplinary in that it takes its sources and background assumptions from the fields of computer science, telecommunications, computer security and human-computer interaction, and even from sociology, psychology, and philosophy. The main application area of the study is ecommerce. However, the users are investigated mostly as *users*, not so much as *consumers.* This means in practice that e.g. methods of areas such as marketing research and economics are not at the core of this work, even if work from these areas is touched upon occasionally. Furthermore, the viewpoint is that of a single user interacting with the system, not users acting as a tight group in a cohesive manner.

The aim of this work was to see, what and how can be found out about trust in the online environment, and which usability and UCD methods provide what kind of results. The goal was to be able to show, how and when these methods should be applied. The goal of this work was thus not to create a generic framework of trust, since such frameworks already exist, e.g. (Riegelsberger 2005), (Jarvenpaa and Tractinsky 1999, 2000), (Gefen 2002), Camp (2000). The aim of this work was also not to provide generic guidelines for creating trustworthy design, since this has already been done quite well by e.g. Egger (2003) and Camp (2003b). However, this work is a) corroborating the results of these two works via a different set of methodology and b) concentrating on showing how different types of usability and UCD methods can be applied in the various parts of trust-formation online. The work can be seen as a continuation of the work conducted by Jarvenpaa et al, adopting a similar line of study especially in regard to the multi-cultural issues, as well as what comes to the chosen methodologies and setting of the research questions (Jarvenpaa et al 1999, 2000).

1.2 The chronological line of research

This work is based on nine publications that present various approaches to the concept of trust from a user-centred viewpoint. One aim of this work was to see how the existing usability methods can be applied to the field of usability in computer security and what kind of information they produce. The publications draw a logical and chronological outline from the initial, general-level user interviews on trust issues through actual usability testing of security user interfaces to analysis of the conclusions and results on a general level. The work also presents a review of the previous work on this topic.

The purpose of the first user study was to find out about trust in the form of enquiring about users' current understanding of the security of the Internet as well as to learn about their behaviour patterns concerning their usage of the Web and areas that seemed relevant to this usage. These include areas such as use of e-mail, use of banking services, and use of credit cards. As our method, we used qualitative user interviews. The users were also presented with a mock-up user interface for a web-based service (group 1) or with existing web services (group 2), in order to trigger conversation about ecommerce and security issues related to the transactions of money or private information online. The users were inquired about their current knowledge of computers and banking habits, in order to find out about the possible similarities in behaviour in the case of using money regardless of the media. The notion of trust was discussed upon on many levels, including questions about trusting friends, work colleagues, a bank or a service-provider on the Web.

The first user interviews and evaluations (group 1) took place in June 1999 and the second in September 1999. In-between the results of the first user study were analysed and compared with existing literature. The second set of user interviews (group 2) was then planned with the alterations mentioned above. These user studies are reported in [P1]. The ethical implications of promoting trust were discussed in [P2], and the whole research setting of bringing human trust closer to machine trust was discussed in [P3].

In order to see if the results would be valid in another country, and also to see how cultural variation might take place, the user study was repeated in Sweden in 2000, with slightly different user group, different sites familiar to the Swedish users, in Swedish language, and by Swedish collaborators. The outcome of this study was that there was indeed quite a lot of difference which is likely to stem from cultural variation, but due to the different user group these results can only be considered as indicative. The Swedish user study is described in detail in [P4].

[P5] presents a concentration on the usability of the actual trust mechanisms currently in use on basis of the findings of the user studies conducted. [P6] reports the resulting UI design built on basis of the research, and the outcomes of the usability tests conducted on this design. The significant findings on the importance of aesthetics for the trust-making decision, as well as an elaboration on how to deal with the different tastes and likes behind aesthetic evaluations are discussed in [P7].

To further test the effects of culture on trust-formation, the original user study, with some slight moderations and with a smaller user group, was again run in Iceland in 2000. Now, the cultural variation seemed even stronger and the trust-formation process appeared to be quite dissimilar from that of the Finns and Swedes. The outcomes of this user study are reported in detail in [P8]. [P9] represents an attempt to further analyse and categorize the findings by applying a semiotic analysis to the identified trust-building elements in the online environment, to understand the mechanisms behind their interpretation in online situations.

On basis of the user interviews we also made a checklist of design qualities that could help to create trust in the user towards the service, even if providing design guidelines was not one of the initial goals of the work. The checklist was on rather high level of abstraction, but could still be used in the actual design of a user interface for a web-based service to ensure the users of the security of their transactions on that service – it could be used to guide the design intended to create trust.

1.3 The structure of this work

The structure of this work is as follows: first, there is an outline of the research questions and methods. Next, a cross-section of work done in the area of usablity of security is provided. The work then proceeds by presenting related work in the area of trust. The work continues with a summary of the main contributions of the thesis, originally presented in the publications that form the corpus of this thesis. The work ends with some concluding remarks, together with presenting some items for future work in trust research.

2 Research questions and methods

This section presents the research questions that motivated this work, together with the chosen methodology, with reasons behind choosing these methods.

2.1 Research questions

As already stated above, the work presented here can be seen as a continuation of the work conducted by Jarvenpaa et al, adopting a similar line of study especially in regard to the multi-cultural issues, as well as what comes to the chosen methodologies and setting of the research questions (Jarvenpaa et al 1999, 2000). These publications report on studying

consumers' online trust behaviour in three different cultures: Australian, Israeli, and, later, Finnish. This ground-breaking study that was one of the first of its kind, showed how trust could be studied, what kind of hypotheses could be built and tested, and also that cultural factors clearly played a role even in a global environment that the Internet essentially is.

Another study closely related to the study at hand is the relatively often-cited research report "Ecommerce Trust Study" (Cheskin 1999). In this work, the central research questions revolved around the definition, development, and the components of trust and trustworthiness, with a special focus on how these might be applied to ecommerce. The research reported here was outlined and started before the Ecommerce Trust Study appeared, which means it had no effect in the design of this study in the first phases. Further, the emphasis in this study was less on the commercial questions and more in understanding and analysing human behaviour in situations involving trust decisions from a usability point-of-view, and on what is the role of trust in both human-human and human-machine interactions in an ecommerce setting.

The research at hand continued and complemented these research approaches by concentrating on finding answers to the following questions:

1. **Sources of trust**

- What are the sources of trust? Is it social networks (family, friends, colleagues), different mass media (television, radio, Internet, newspapers, magazines), or some other?
- What is the relative importance of these various sources for trust forming?
- In what kind of situations (email, ecommerce, online bank services) do users feel that trust is an issue? How do they express this?

2. **Definition of trust**

- What do users mean when they state they trust or distrust someone or something?
- How can the implicit meanings of trust be made explicit? Can this be done?
- Are there different levels of trust? If so, can these be defined somehow?

3. **How to express trust?**

- What ways of visualising trust would be acceptable and understandable for the users?
- What would not be acceptable?
- How much of trust management can be automated, and how much should be shown to the user?
- In what format and how much information about security should the users be provided with?

4. **Finding the right technology**

- How can users' expressions of trust be mapped with existing security technology, or,
- Should a new set of security technologies be created "from scratch" that would better take into account the novel uses (e.g. ecommerce) and novel users (i.e., the technologically ignorant)?

The research questions were chosen on basis of the previous work by Jarvenpaa et al as cited above, and also based on a literature survey performed before planning the user studies. Further, the needs discovered in the previous work in the research conducted in the area of computer security in the research projects at the same university, especially the work by Nikander (Nikander 1997, 1999) influenced the problem setting. The scope of the research was reformulated and updated against the gathered data, as well as on basis of the outcomes

of the Ecommerce Trust Study, in an iterative fashion, concentrating on issues that seemed most relevant in the light of the findings.

2.2 Methods

In the Ecommerce Trust Study, the research methodology included qualitative questionnaires, site review and analysis, expert opinions, and consumer opinions, neither of which was, however, conducted face-to-face (Cheskin 1999). As already mentioned, our studies were initially planned without knowledge of this study existing. In our studies, we wanted to try a different methodology than was used in Jarvenpaa et al (1999, 2000), since in their studies, also Finnish users had been involved so a different kind of approach would serve as complementary. We chose to use a more qualitative, or "soft", approach, stemming from the HCI and ethnography: interviewing, observation of behaviour, and UCD and usability testing. These chosen methods are among standard means of gathering data about users inside HCI, so their selection is well grounded in that respect also.

Choosing the right method for study depends to a great deal on the research questions and on the goal of the research (Landauer 1997). As the goal here was to enhance the current understanding a broad and ill-defined concept, such as trust essentially is, interacting with users face-to-face, interviewing and observing them seemed to be the approach that would most likely produce the kind of research data we needed. This point is further emphasised by the fact that trust was to take place in such a broad and equally ill-defined environment as the *online* environment is: Finding out what users actually mean when saying they trust something and how this trust might be expressed in practice in online situations, was likely not be to straight-forward. The choice of the methodology seems successful in that respect that some of the methods were similar to those of the Ecommerce Trust Study, providing a basis for comparison for the outcomes of the studies. Also later on, the research approach of B.J. Fogg and his group at Stanford (Fogg 2003), who also involved Finnish users in their study, became another complementary source for validating the results of our studies. This study used as main source of information online questionnaires, and is explained in more detail in later chapters. The emergence of studies with more or less the same research questions, but with a different set of methods, enabled comparison across the methodological theme of the work at hand: what kind of research approach would be most suitable for studying trust in the context of users' interactions in the online environment?

2.2.1 Semi-structured interviews

Asking users directly on the topic is usually not a good idea, unless the aim of the research is to hear what the users consider as ideal behaviour under ideal circumstances (Keats 2000). Users tend to give "school class answers" to direct questions, describing schematized or ideal behaviour, instead of describing how they actually behave in real situations. This is why usage of questionnaires was discarded, especially since such research exists (e.g. Fogg et. al. 2000 onwards). It is also quite hard to design a good questionnaire on such a topic as "trust" or "usable security", with which so much remains not properly understood. Qualitative, semi-structured interviews, on the other hand, seemed a good way to make users discuss such issues, since it allows for real-time reactions to the answers received, as well as for probing (Keats 2000, Kapaki et.al 1997). Further, since trust issues can be rather emotional and private by nature, the rapport built during the interviews would provide for depth in the answers and discussions that might not be possible to achieve through other methods (Keats 2000, Landauer 1997), thus complementing and opening the results gained by using questionnaires for further analysis also.

Since most users are either not familiar with security issues and/or do not think of them in abstract terms but rather in relation to some experiences they have had in using applications or systems where security has become an issue, the interview structure was built around such areas that were thought to be familiar to the user. In this case, use of email, use of online bank services, and use of ecommerce are this kind of use areas that users were familiar with. There is a double idea hidden in this design: firstly, users are, in general, more interested in what they can achieve with new technology instead of being interested in the technology itself. People care for the *goal*, not for the means to get there (Adams and Sasse 1999b). The same goes for security: it is not an end in itself, but rather means to an end: a way to send and receive private email; to be able to find bargain prices for commodities in the Internet; to handle banking affairs safely from the home, and so on. This is why if we asked people directly, what they think of security, they might answer they *don't*. However, users may, in fact have many ideas *related* to security that have arisen from previous usage of security-critical systems. It is the researchers' job to induce this level of analysis and find the right information from it (Landauer 1997).

Secondly, people tend to be a bit of afraid of technology they do not understand, and computer security definitely belongs to this area. This is why people can easily feel that they do not know anything about security, and have no real experience of it. In fact, when looking for the non-technical, inexperienced users for our studies, we had a hard time convincing our users that it really was "ok" not to know anything about security and yet be part of the study. In general, users want to be successful in the studies; they want to perform well (Landauer 1997). They are afraid they will look foolish, if they feel they do not have enough knowledge about the problem area under study. However, when users are asked about areas that are common to them, such as use of email, they tend to be happily surprised to find out that in fact they, in a way, do know about security, and more, they even have opinions about it. Therefore, a lot depends on how the questions are phrased and presented to the users, and the possibility for probing seems crucial to the relative success of this undertaking. In our case, it was often sufficient to convince a hesitating user to participate by asking: "Well, have you ever used email? Yes? That is enough!", or, "No? Have you used Internet? Yes? That is enough!"

The user interview basic structure is presented in more detail in the **Appendix**.

2.2.2 Evaluating existing services

Just talking about the matters in an interview is most likely not comprehensive enough, since, as is well known, users often say one thing and do another (e.g. Landauer 1997). To get the real picture of how users really might behave in situations where trust is in issue, it is better to put them in that situation and then have them act on it, rather than just discuss it in theory. Such a setting was accomplished by presenting users with a mock-up UI design for an online service (the first user study, group 1) or with existing Web services to go through (the second user study, group 2).

After the interview section, on areas related to trust and security as described above, the users gained some tasks to perform with either the mock-up (groups 1) or the existing Web services (group 2), to find, identify and discuss the security features of the tested application or services. In the latter case, the users were also requested to evaluate the Web sites focusing on their apparent security.

As the users went along conducting these tasks using the talk-aloud protocol (Nielsen 1993), the up-coming issues were discussed with the interviewer. After testing the application or services, the users were again interviewed, in the form of a semi-structured interview. Probing was used when users gave elusive answers or when users gave an answer that could be used

to lead the discussion to a deeper level. The interviews in all were taped with the users' permission, to guarantee for exact recall to avoid subjective bias as far as possible.

The basic structure for the evaluations is presented in the **Appendix**.

2.2.3 User-centred UI design and usability testing

User-centred design (UCD) starts with setting the user at the centre of attention and in control of that attention: UCD is based on the idea that the user knows what is best for him. Users are the best experts of their everyday life. This is true to the extent that the needs and the desires of the user must indeed be taken from the users, not invented by the designers and system builders, for example. On the other hand, it is not right to expect user to be clairvoyant about either his own unconsciousness nor about the future. It is not user's responsibility to analyse the needs behind perceptible behaviour; nor be able to foresee new product ideas embedded in the lackings of the current situation and enabled by new technology and the minds of innovators – even if sometimes users can be quite innovative, too. Borrowing a felicitous example from (Karvonen and Parkkinen 2004) describes the setting in UCD quite well:

> *"Asking the user what he would like is like asking him to describe ice. A person can usually describe the common properties of ice such as its temperature and moistness. Some people may portray the benefits or uses of ice, such as winter sports or cooling a drink. Few people are able to innovate new ways of utilising ice. However, when a designer comes up with a new and exciting idea such as using ice to cool feel on a hot summer day with special-made shoes with ice within, the idea and its benefits for the user must be measured before intitating mass production. This is the phase where UCD methods can provide the designer with tools to communicate with the future users of ice shoes. A designer living in a hot area may well come up with the idea of ice shoes, but a designer living in a chillier climate is likely not to be familiar with such a need as cooling one's feet before getting to know the users of hotter climates."*

Applying UCD means in practice that the user requirements are considered right from the beginning and included into the whole product cycle. The major characteristics in UCD are the active participation of real users, as well as an iteration of design solutions. This approach is manifest throughout the research via user interviews, as e.g. in [P1], user evaluations [P1], [P4] ,[P8], and usability testing [P6]. The usability framework is based on the International Organization for Standardization standard ISO 9241-11:1998, Ergonomic requirements for office work with visual display terminals (VDTs) – Part 11: Guidance on usability, where usability is defined as consisting of

- Efficiency,
- Effectiveness, and
- Satisfaction.

In all, usability, the usability of security, as described above, and UX and emotional HCI research provide the methodological and theoretical background of this work (e.g. Norman 2004).

3 Background

In this chapter, we will have a look at a cross-section of work done in the area of usability and security.

3.1 Usability of security

The goal in studying the makings of trust and usability of security in general, is to overcome the problems identified above so that in the future, the actual and the perceived security of, say, a web-based service, would be the same, and computer security would be seen as usable, understandable, maybe even enjoyable. In order for this to happen, a lot needs to be done. But how can we do this? How can we make such security more usable? The current low level of the usability of security can be said to stem from two different sources. Firstly, these systems and applications were designed for the technologically advanced, so their user-friendliness was not an issue: all the users knew the relevant terminology and what was going on behind the UI. This means that from the average man's point of view the current UIs are still full of technical jargon, difficult to understand and to use, and not enough appropriate help is provided, even when the user population has greatly expanded and become more and more heterogeneous when it comes to the technological know-how the users possess. Secondly, there is a lack of interest, or motivation, for security: users are not interested in these systems as an end in itself, but only as means to some other goal. The current user population is not interested in the security behind the scenes, only in knowing that it's there and what it enables. So, every task the users have to take to ensure their security is a pain. Any attempt to raise the level of usability of security should, then, take into account both of these affecting factors in order to succeed.

Partly due to the common disinterest towards computer security, partly due to the inherent complexity of the area, an often suggested answer to the problem of low level of usability within computer security is to increase the automation level of security. In this scenario, security would be taken care of by the system on behalf of the user, and the user need not bother about it. However, for example in a now classical study on the usability of PGP 5.0, Whitten and Tygar (Whitten and Tygar 1998), state that even though automation may be the right solution for securing the communication channel itself, there remain situations where automation is not, and cannot, be the answer. At many points manual handling of the security features is required from the user, for example when giving access to shared files for others.

Also, hiding security completely from the user is not a good idea for other reasons as well: if the security mechanisms are totally hidden, the users are not able to tell whether they are working or not, which would allow for successful attacks to remain undetected and make the system insecure (Jøsang et.al. 2001). Also, users have a need to be able to perceive that security is in fact taking place – they need some kind of feedback (Adams and Sasse 1999). Users also have a need to feel in control when using the system – so full automation is not the answer they are looking for (Cheskin 1999, [P1], Nielsen 1999). Shneier states that security is easiest when it is visible to the user, when the user has to interact with the security and make decisions based on it: checking the name on a digital certificate, for example (even though making the concept of certificates understandable to the users may prove tricky, as we have experienced in [P6]). On the other hand, also Shneier is aware that users do not want to see security, they just want to know it is there (Shneier 2000).

An important thing to emphasize is that people do want security, but they do not want to see it working. People are ready to compromise their security if it "gets in the way" - when something needs to be done quickly, they give up their security to get there. It is a trade-off between easy flow of action and having security. Once people want something badly enough, they forget about security precautions (Shneier 2000, [P1]. In a way, security can be easiest when it is visible to the user, when the user has to interact with the security and make

decisions about it. However, our studies have shown that users do not actually want to see security – it either frightens them or bores them [P1], [P3].

Some information and evidence about security taking place should, then, be provided. However, it is essential that this information be presented *in the right way* to the user, that is, in a way *understandable* to the user. How to be successful in this is to use real users as evaluators of real and/or planned systems. A good example is easily found: In their evaluation study of PGP 5.0, a trust management system rather widely used and usually considered to be user-friendly, Whitten and Tygar found that the graphical user interface of the system was not, however, easily understandable to the users, and thus its functions were misunderstood and misinterpreted (Whitten and Tygar 1999).

On basis of their research Whitten and Tygar claim that ordinary usability measures are not enough for ensuring the usability of security – the basic principles that had been used to try to make the design more user-friendly. Because of this, they set forth their own definition for it. This definition consists of rather general statements on how users should be made aware of the security tasks at hand, of how the users should be guided through the procedure, dangerous errors should be prevented, and the use should be made as comfortable as possible. These requirements seem rather commonplace for any usability expert, the only major difference to "ordinary usability" – in the sense of effectiveness, efficiency and user satisfaction (e.g. Nielsen 1993) – being in the *irreversibility of error-making*: if the system security is lost once due to an error, it may be lost forever. This is an important – and novel – point indeed.

More interesting, however, is Whitten and Tygar's analysis of the problems typical of security. These include lack of motivation for security, the abstractness and *alieness* of computer security management systems for average users, lack of feedback, and, again, the importance of not making any mistakes – the use should be free from at least dangerous errors, or else the whole integrity of the system is at risk.

In the usability study of the KaZaA P2P file-sharing system already described, replicating the methodology in Whitten and Tygar's study came up with similar results (Good and Krekelberger 2003). In this study, Whitten and Tygar's usability demands for computer security were slightly modified. Good and Krekelberger laid down four demands for Peer-to-Peer (P2P) file sharing software to be safe and usable for its users. These demands were

1. Users are clearly made aware of what files are being offered for others to download.
2. Users are able to determine how to share and stop sharing files successfully.
3. Users do not make dangerous errors that can lead to unintentionally sharing private files.
4. Users are comfortable with what is being shared with others and confident that the system is handling this correctly.

Even when these demands sound very basic, in the mentioned study the KaZaA system failed in all of them. According to (Zhang et al 2005), the distinguishing concept in P2P systems is *sharing*, by contributing to and benefiting from the Peer community (Schechter et al 2003) A fundamental problem in P2P systems is how to ensure and verify the authenticity and integrity of shared data or communicated information in open and highly distributed environments. Currently, most existing P2P applications do not have mechanisms to address these problems. From the usability point-of-view, the *extent* of sharing presents a further problem, as we have seen.

Adams and Sasse (1999b) also give recommendations for creating usable security in their treatment on how to make passwords user-friendlier. Even if the emphasis in their work is in password usability, they also give recommendations on how to make computer security in

general more user-friendly. Motivating users, giving feedback and providing guidance come first on their list of design requirements as well. Further, Adams and Sasse also emphasise the importance of *showing* the users that security is taking place: "System security needs to be visible and seen to be taken seriously by the organisation" (Adams and Sasse 1999b).

Adams and Sasse emphasise the organisation's responsibility in creating an atmosphere where security is considered important and worthwhile. Better password usability is certainly crucial for increasing the usability of security, and this is, in fact, one of the areas of computer security where there exists some user studies already (e.g. Adams and Sasse 1999b, Dhamija 2000, Bunnell et.al 1997, Brostoff and Sasse 2000). Also Sandhu (2003) makes good comments on this issue on organizational password policies being cumbersome and ungrounded. However, password usability falls out of the scope of this study.

According to Shneier (2000) there are several features in handling security that make it special from other usage situations the user might come across. These include risks and exception handling. There are risks that people do not understand and whose impact they cannot estimate, nor predict when they might take place. Giving additional information to the users does not usually help, since this information is often too complicated, and even after understanding the information given, it may still be difficult to judge whether the risk is realised in the special case at hand or not. (About risks see also (Camp 2000)).

On basis of these observations, Shneier has come up with a list of the six corner stones of the "human problem" in computer security:

1) how people perceive risks
2) how people deal with things that happen very rarely
3) the problem of users trusting computers, and why that can be so dangerous
4) the futility of asking people to make intelligent security decisions – they cannot always do so
5) the dangers of malicious insiders, who are trusted implicitly
6) social engineering, and why it is so easy for an attacker to simply ask for secret information, e.g. over the phone.

On top of all these problems, a further complication with security is that it is about probabilities only; there is no absolute guarantee that security *de facto* happens. All security systems that are currently known are breakable – at least in principle. In most use cases where security is an issue, the most effective methods of securing the transactions taking place is not the heaviest method, since these take up a lot of processing time. In addition, the case where security is at risk is when a mistake occurs where there usually is no mistake. This means that since mistakes are "too" rare, people do not know how to deal with them. Usually things proceed "ok" – everything goes as planned. When an error occurs, it is unexpected, and users' have no idea as of how to deal with the problem. It is very time-consuming to start looking for advice. People do not know where to find it, and even if they do find it, they do not always understand it, and often they are in a hurry and need to get things done. The usual trial-and-error learning method so much in use with current information technology does not work with computer security, where even one mistake may be too much and end up in compromising the security for the whole system from then on. In this sense, at least, there seems to be a clear deviation from the standard usages of computer systems.

This is related to the concept of "good-enough security", the idea that perhaps it will not be needed to be able to guarantee absolute security, after all, but lesser means would be satisfactory – and safe – enough. Sandhu (Sandhu 2003) calls the "three golden principles" to guide information security the following:

- Good enough is good enough.

- Good enough always beats perfect.
- The really hard part is determining what is good enough.

Referring to the words of Albert Einstein, “Everything should be made as simple as possible, but not simpler”, Sandhu suggest the following adaptation for the information security business: “Everything should be made as secure as necessary, but not securer.” He sees this as the essence of good-enough information security. While he acknowledges that there probably will be security fundamentalists who might question whether this is a reasonable quest, he clings to his claim. Sandhu refers to the networks currently in use that have good-enough security, namely the system of automatic teller machines (ATMs), where security is not absolute and still for the most, this is enough and users are usually comfortable using them. Since security goals have inner contradictions because confidentiality, integrity, privacy, accountability, and recovery often conflict fundamentally, according to Sandhu it makes no sense to strive to demand for perfect security, since it is probably not possible anyway – and the users are not asking for it, either.

One more typical thing in usability of security is that even when the user knows what he or she wants, it is no easy task to transfer this goal to the computer so that it will do what the user wants it to do. The fundamental problem is that users have no idea what the computer is actually doing when they tell it to do something. This became painfully obvious in the aforementioned usability studies of PGP 5.0 and KaZaA as well: users were assuming their files were safe and emails encrypted, when in fact they were not. However, users do not, in general, have enough information nor skills to be able to judge the situation right, and if they want to go ahead with e.g. their file-sharing or emailing, they just hope and trust that the system is doing what they want it to do. A leap of faith is required from the user – trust is needed ([P3], Shneier 2000).

People’s needs for security may also differ. For example, when it comes to privacy, Shneier states that people have a complicated relationship with privacy: When asked to pay for it, they often do not want to pay; they will rather do without – mainly because they may not understand how much is at risk. Cranor et al have stated that people can be categorised into different groups according to the level of privacy they need (Cranor et al 1999). However, people are not always aware that there is something to lose when giving away their privacy. Shneier goes as far as to claim that almost no-one realises exactly how important privacy is in his or her life – before it is gone (Shneier 2000).

Another thing affecting the usability of security is *anonymity*. In most cases, when we are making transactions online, taking part in chat and news conversations, we may be identified by others. There are two schools of thought about this: those in favour of strong authentication, where users are always identified, and those in favour of anonymous authentication, where users are only identified to have a right to a certain service, but not identified as who they really are. However, do we need anonymity? Is it a good thing or not? How do users feel about it? This is a question that is clearly related to the privacy categorization by Cranor et al, and it is likely that here people’s preferences will vary. However, in certain situations people might differ not so much at all: e.g. Social anonymity (e.g. help lines), as well as political anonymity certainly seem to be needed also in the future, both in networks as in real life (Fukuyama 1996, [P3], Shneier 2000).

However, providing means for anonymity online may have its side effects: people are already using the anonymity on the Internet to also send threatening email, publish hate speech, disperse computer viruses, and so on (Shneier 2000). Authentication is needed on some level: it is about the continuity of relationships, knowing who to trust and who not to trust, making sense of a complex world. If there is no way to authenticate the service provider, how does the customer know whether to trust the service provider? Which of the merchants are honest, and which are scams? The Web-site name may be well-known outside the Web, but is it

really the same merchant (Shneier 2000)? These questions are related to the problems of identity management, where there remain many unresolved usability issues, as well as an important threat for trust creation, namely *identity theft*. Identity management, however, falls out of the scope of this study, though its relevance is immense (c.f. Camp 2004 for a good presentation on the topic of digital identities).

According to Shneier, this is the most difficult problem to solve: authentication across digital networks. There are going to be as many different solutions as there are different requirements. Some solutions are going to have to be robust, protecting values in the millions of dollars. Some do not have to be so strong: authentication for a merchant's discount card, for example, and so on. Which of these does the user need to be able to use and understand, and which will be acceptable for which user? These questions urgently need answers. A further problem with authentication from the control point of view is that often computer authentication is, in fact, invisible to the user. For example, when a mobile phone is used, it authenticates itself to the network so the network knows whom to charge for the calls. This authentication might be unwanted – at least as strong authentication, e.g. the user might not wish to leave traces of his or her movements on the network.

It has also been argued that the real problem is not at all in finding reliable encryption and authentication methods, for these exist already: the problem would then not be in the secure technological infrastructure, but more so in creating enough trust in users towards these systems and thus increasing their willingness to indulge in the transactions over the Internet via reducing the amount of perceived risk involved in such transactions (e.g. Salam et al 2003). This could be achieved through various means, such as using TTPs as intermediaries, for example.

However, from a user's point-of-view, authentication is just one question among many. A further problem with usability of security is to define the right level of information provided. In the case of trust, it seems we have two options: either we can hide the security features from the users as fully as possible, or we must make them understandable from the user's point-of-view. As we have seen, full automation is probably not the best possible approach to induce trust. A mixture of hiding and revealing information about the security, along with preventing the user from making any serious mistakes, is a likely solution. It would also be worthwhile to see if it would be possible to vary these features according to the amount of use experience the user has, by providing less choice for novice users, and more flexibility for experienced users, as their trust requirements are likely to be different: experienced users with an understanding of the technical features of security will want to have access to that information in order to be able to trust the service built on that technology, whereas novice users will shy away from instructions that appear to be too technical and avoid overflows of such information. Knowing the users and which user group they belong to, is key in being able to create a successful mixture of hide-and-reveal approach to visualising computer security on a user interface level.

One more thing to consider is that some of our "users" who need to trust others may actually not be human users, but might be other computer programs, servers or companies. However, the use situation remains the same, so it may be a good decision to hide this variety of users from the novice and intermediate users, at least to avoid confusion. From the user point of view there is no real difference in the operations, whether performed by another human user or by a machine granting or revoking the rights, so there should not be a difference on user interface level either.

What we have seen is that "usability of security" might indeed be somewhat different from "ordinary usability". The major difference seems to lie in the *risks* entailed in computer security – error-making has much more powerful repercussions in security than in most other computer-related areas involving users and/or user interface design. Complete avoidance of

user-made errors is a novel demand introduced by usability of security, and it is likely to be a hard nut to crack. In other appliances, like surfing on the Net with a graphical browser or using a word processor, a trial-and-error method is how the rules and logic of these systems are learned. Making mistakes might be frustrating, and time-consuming, but it does usually not create any major risk. With computer security, however, the situation is altogether different, as we have already stated. It is a good question, then, how we are going to deal with this high demand on error-freedom. Since most graphical user interfaces the users are currently familiar with allow making mistakes, it might be a good idea to base the design of security user interfaces on a completely different UI design principles, and try to *avoid* any similarities. As surprising as this suggestion may seem, it might in fact be the only way to stop users from learning the use of the security UI through the trial-and-error procedure they are used to revert to with the introduction of other applications used with the same device. The downside of this approach is, of course, in that it requires an extensive amount of learning effort from the users, not to mention motivation – which we have already seem to be low in matters of security (Adams and Sasse 1999b). What seems to be certain is that one ingredient in making computer security more usable and what such user interfaces should achieve is enhancing the system's capabilities of appearing trustworthy, and the way it can enable users to express their trust in a way that seems natural to these users.

It is characteristic of usability of security research that it is still rather scarce, though its importance is recognised and acknowledged. Recently, more and more work has however started appearing in this field, including some summaries on this work (e.g. Cranor and Garfinkel 2005, Riegelsberger et al 2003, Camp 2001, Araujo and Araujo 2003, and Ellison 2002, Dourish et al 2004, and Grinter et al 2005 on security issues at homes, etc.).

4 Related Work

In this section, we will provide a representative sample of various types of trust studies that exist, starting with various ways how trust can be defined, and phrasing our own definition for trust. This is followed by presentation of a selection of ways trust has been studied, divided into subchapters. The treatise of trust research is by no means intended as exhaustive, since this would in practice be impossible – its aim is to cover the classical studies in this area, but also to show, via selected examples, the great variety of approaches in existence in trust research.

4.1 On the concept of trust

It is difficult to think of a research topic more intriguing and difficult than "trust" essentially is. It has been studied from each and every angle: in the philosophical, sociological, psychological, computer scientific, economic, and legal sense – just to name a few. Alas, not many firm and unifying results have been reached so far, and not much uniformity in how to define the concept of trust, in the first place, has emerged. This is regrettable, for trust is nonetheless seen as one of the very bases of online interactions, and further, the very basis of our society.

The very meaning of the term trust is itself problematic and often unscrutinised, and there are many alternative definitions of the word. Again, the Thesaurus provides a partial answer: with trust, we can mean, among other things, "complete assurance and certitude regarding the character, ability, strength, or truth of someone or something". As synonyms for trust, we get a list including concepts such as confidence, dependence, faith, hope, and reliance. We also get a list of related words – these have something to do with the notion of trust. The list is made up of assurance, certainty, certitude, conviction; belief, credence, credit; positiveness,

sureness; entrustment; overconfidence, and oversureness (http://www.m-w.com/dictionary.htm).

Even if the Thesaurus gives us some understanding, it is by far not enough. Trust is a complex phenomenon that has up-to-date not been analysed properly either in philosophical, sociological or technical sense of the word. Trust has sometimes been defined as something that "begins where prediction ends" (Lewis and Weigert 1985b) and is often considered to be little more than an individual psychological state that has more to do with a specific individual and her psychological and sociological make-up than with some real-life state of affairs (Lewis and Weigert 1985a).

Sociologically, trust could be defined as a sort of a "header" that describes the nature of transactions between two or more individuals, an individual and an institution or an authority, or between two institutions, to put it in a simple way (Giddens 1989) – interactions happen in a trusting atmosphere. A sociological study of trust would concentrate more on the distinction between trust in people and trust in "abstract systems", and interpersonal trust is built upon mutual involvement and in the faith in the integrity of the other person. Trust in the abstract systems, however, is the basis for feeling of day-to-day security that in its turn forms the basis for social life (Giddens 1989). This trust in "abstract systems", or, a trust in an impersonal, anonymous someone seems to carry some similarity as compared to the current situation of trust in anonymous service-provider on the Web – an abstract system from the user's point-of-view.

Trust can be also viewed as a historically emergent property of human interaction that is tied to a specific form of social organisation (Lewis and Weigert 1985b). Modern forms of trust are, then, rooted in the rights, obligations, and liberties of citizenship (Lewis and Weigert 1985a, Fukuyama 1995, Luhmann 1979, Seligman 1997, Loukola 1999).

Philosophically, trust is to be separated from confidence and faith – both concepts with which the concept of trust seems to be at least partially overlapping (Seligman 1997). Trust is related to all these concepts and must be set in context with them. However, a further philosophical analysis of the notion of trust falls, again, out of the scope of this study, even if trust has traditionally been dealt more by philosophers than social scientists. Among the latter, trust has been explored mostly by social choice theorists (more specifically, usually through the development of Prisoner's Dilemma games, (e.g. Loukola 1999)) and as large-scale surveys on existing literature on "trust" in local and national governments, NATO, the UN, etc (Seligman 1997). It soon becomes obvious that the use of the term trust tends to be loose and imprecise as it ranges from micro to macro encounters and is used to express ideas akin to Durkheim's solidarity on the one hand and simple confidence in the iteration of interaction on the other, and everything in-between: trust is hard to pin down to an unambiguous definition.

This variety for the meanings of trust we have just witnessed should come as no surprise, for one already can intuitively feel that the "trust" existing, say, between members of a relatively undifferentiated, tribal society may be of a very different order than that bestowed (or withheld) among modern, contracting, market-oriented individuals, citizens of nation-states. Among these latter, the obligation to be trustworthy, and so to fulfil promises, arises from the moral agency and autonomy, from the freedom and responsibility, of the participants to the interaction (e.g. Fukuyama 1995). Moreover, without the prior existence of these conditions, rights really – rights to freedom, autonomy, and responsibility, the moral dimension of promise-keeping, and hence of trustworthiness – cannot be adequately explained (Seligman 1997). In fact, the structure of our civil society as it now appears to us, is based on such various trust relationships and expectations (Fukuyama 1995). Indeed, the existence of trust is an essential component of all enduring social relationship: power, dominance, and coercion can be a temporary solution to the problem of social order, but they will not provide the basis

for a permanent solution, or maintenance of said order over time – only social trust can do this (Seligman 1997).

The same goes for the "online order" – the same rules of human order and existence apply. Real-world trust seems to be transferable to the digital world: Trusting a bank stays more or less the same regardless of the media (e.g. Ecommerce Trust Study 1999) (there are, however, also some reports on studies that disagree on this point, e.g., Hoffman et al 1999). More important than the place where the service is situated seems to be the existing brand reputation and other users' opinions about the service provider. These elements create the *sense of place* that guides the social interactions, perception of privacy, and the nature of all transactions conducted online (Adams and Sasse 1999b).

In brief, it can be said that while some form of trust - or more properly confidence - among social actors is necessary for the continued operation of any social order, the issue of trust as a solution to a particular type of risk is, according to Seligman, a decidedly modern phenomenon, linked to the division of labour in modern, market economies (Seligman 1997) – a solution that should now find ways to transform into online trust as well.

Further, trust, as both a solution to and an articulation of a specific interactional problem, is tied to a particular idea of the self that we identify, most broadly, with modern social formations (Seligman 1997). On the most general and abstract level it can be stated that the need for persistent, stable, and universally recognised structures of trust is rooted in the fundamental indeterminacy of social interaction. This indeterminacy lies between:

- social actors,
- social actors and their goals and
- social actors and results.

Furthermore, this indeterminacy results in a basic unpredictability in social life notwithstanding the universality of human interdependence. So, any social structures intended to have any permanence over time must be based on developing mutual trust between social actors: trust enables them, sustains them and enhances them (Seligman 1997).

The emphasis in modern societies on consensus, the ideology of pragmatism, problem-solving, and technocratic expertise, as well as conflict management, are all founded on an image of society based on interconnected networks of trust – among citizens, families, voluntary organisations, religious denominations, civic associations, and the like. Similarly the very "legitimisation" of modern societies is founded on the "trust" of authority and of governments as generalisations of trust on the primary, interpersonal level. Also, the definitions of trust in Western industrialised and "modern" societies are rooted in the idea of the individual as final repository of rights and values (Seligman 1997).

From a cognitive point-of-view, trust seems to imply lack of sufficient amount of knowledge (Adams and Sasse 1999b, Safer Internet 2006, Cardholm 1999), meaning that there is at least some amount of uncertainty involved (Jøsang 1998, Jøsang 1999, Mühlfelder et al 1999). What this means from the user's perspective, must be studied further. Furthermore, trusting reduces the complexity of a situation (Olson and Olson 2000, Seligman 1997). When we *decide* to trust rather than suspect — there is *a leap of trust* — the number of issues we have to consider is reduced, thereby simplifying the process of making decisions. How such trusting decisions are made and what they are based on is one issue for further studies. Trusting also describes *an attitude* towards future expectations, as well as introduces the presence of implied risk in a given situation (Mühlfelder et al 1999). How these attitudes are formed is one more relevant area for trust research.

We have discussed on how trust is a notion that frequently comes up in any conversation about creating more usable computer security design (e.g. Anderson 2001). However, what do we mean by *security* in this context, and how are the concepts of security and trust interrelated? A Thesaurus tells us that security is linked with such concepts as "safe", "reliable", "stable", "sure" or "riskless". Looking at security from a more technical point of view, security seems to be made up of the ingredients of confidentiality, integrity and availability (White et al 1996). Confidentiality here means privacy: the information transmitted between two systems is revealed only to authorised individuals. Integrity, on the other hand, is protection of transmitted data from being transformed in any way. The meaning of availability is intuitive: it means that the data is available to authorised users whenever they need it (Holmström 1999, Anderson 2001).

Trust is related to such neighbouring concepts in computer security as confidentiality, secrecy, and privacy. On basis of (Anderson 2001) these terms may be further shortly defined (from a technical point-of-view) as follows:

- *Secrecy* is a technical term that refers to the effect of the mechanisms used to limit the number of actors who can access the information at hand. Such mechanisms include use of cryptography and/or computer access controls.
- *Confidentiality* involves an obligation to protect some other person's or organisation's secrets. It is like a 'promise given' not to disclose such information to others.
- *Privacy* is the ability and/or right to protect one's personal secrets. It extends to the ability and/or right to prevent invasions of one's personal space.

In order for any system to be trustworthy, then, it must include all of these, and to be able to maintain them. In order for the system to be *perceived as trustworthy* from the user-point-of-view, it must also communicate these different sides of its technical trustworthiness to the user in an understandable way.

In the context of humans and technology that we are now in, we need to define trust from a technical point-of-view as well as from a human point-of-view. In the human dimension, the definition of trust is still seeking its formulation as we have just seen, but from the technical side things are a lot easier – we have some basic definitions available. This section is to a great extent based on [P3], where it is presented in more detail.

To begin with, in the technical sense a distinction can be made between two basic meanings of trust as an overall characterisation of the whole system. In computer security literature in general, the term is used to denote that something (i.e. a computer system) *must* be trusted (e.g. Trusted Computing Base, TCB). That is, something trusted is something that the users are *necessarily* dependent on. If a trusted component breaks, the security of all of the system breaks. There is no decision of trust to be made, the user necessarily "trusts" the system if he/she uses it in the first place. Further, a separation between *trusted* and *trustworthiness* is made (e.g. Anderson 2001). A system can be (erroneously) trusted, when in fact it is untrustworthy and can fail. However, *trustworthiness* means that the system really is trustworthy and can be trusted: it won't fail (Anderson 2003). So, in the technical world, *trusted* refers to the actual behaviour and attitudes of users, and does not tell us everything (if, indeed, *any*thing) about the actual system, whereas *trustworthiness* refers to the system's attributes, and states the true state of its security. On the other hand, in more psychologically oriented literature, the terms trust and trustworthy are used to denote that something *can* be trusted. That is, something trusted is something that the users *feel comfortable with* to be dependent on (e.g. Nielsen 1999a). If a trusted component breaks, the users feel betrayed. (Probably some harm is done to the security of the system as well, but that is less relevant to this discussion.) This distinction should be kept in mind.

Trust, as a technical expression, is about whether a *subject* (program or person) is allowed (or trusted) to perform a specific *action* on some *objec*t. The question could range from e.g. if user Alice[1] is allowed to read file.doc, to if we can trust a piece of downloaded software to run on our computer (possibly under certain conditions). There has been already a number of various techniques that attempt to express real life trust in various kinds of digital format. *Trust management*, as a component of security in network services, refers to management of security *policie*s, security *credentials* and trust relationships (Blaze et. al. 1996, 1999). A security policy is a formal representation of the allowed (and forbidden) actions in the system. A typical example would be a policy on access control, stating e.g. that subjects with certain credentials are allowed to access some specified objects. More generally, a security policy is a formal specification of authorisation. Credentials are statements concerning a subject made by some speaker, often expressed in the form of certificates, that is, electronically signed documents. A typical credential would be (a certificate stating that) "this public key belongs to Alice". From a user point of view, the trust management level is the security abstraction level that is of interest. Trust management is relevant, when we want to make educated decisions about who to trust, as well as when we make policy decisions concerning, for example, what applications we trust to run on our computer.

In order to clarify things on how trust management in practice works, two different, currently existent approaches to the trust management problem: PGP (see e.g. PGP Users Guide, http://www.pgpi.org/doc/pgpintro/) and PolicyMaker (Blaze et. al. 1996)) were presented and compared in [P3] and [P5]. Both of these also have their own application areas: PGP is intended for providing keys for secure email, while PolicyMaker is a more general framework for trust management.

Both trust management systems presented solve some of the overall trust management problems, but they still have their limitations. PGP is relatively rigid and bound to a single application. Even if it is based on a relatively intuitive trust model, it still has considerable usability problems, and is not intuitive to many users (Whitten and Tygar 1999). PolicyMaker on the other hand solves the problem of being a generic mechanism, but it is clearly intended for the application developer, not the end user [P5]. Also, PolicyMaker leaves it to the application developer to decide how to express trust, which means it is very unlikely that different applications will be interoperable or understand the same policy. (KeyNote provides some improvement on this issue).

However, as has been argued in (Nikander 1999), these systems can and should be, extended to handle also other forms of trusted information. That is, even the expressions of authorisation information may be considered as a form of trust expressions, and the same kinds of certificates can be used to express many other forms of trust. Thus, it can be proposed that some form of authorisation certificates, or rather *trust certificate*s, could be used for expressing *trust decisions* and *recommendations* made by the users [P3]. The certificate-based solution is presented more in detail in [P3]. The problems of revoking such certificates, as well as many practical issues with using certificates remain still greatly unresolved. These problems were touched briefly in (Karvonen et al 2001).

Given this kind of arrangement, users could also express their opinions about specific brands by referring to the public keys of those brand names [P3]. Already as such, these kinds of techniques could be used to create digital counterparts of our real life social networks, and to express our opinions in a digital format.

[1] Alice, Bob, etc. are regular pseudonyms for parties in security protocols. Even if person names are always used, this does not mean that the parties involved are always human – they may be either humans or machines.

The purpose of the explicit utterance of trust, in the form of certificates, is to promote *a climate of trust*, where interactions are based on trusted communication lines and parties, and to create *a secure sense of plac*e, allowing the users to conduct their tasks with a feeling of security that is based on real security measures [P3] As discussed, essential elements in these are good-quality relationships, explicit brand reputation, and other users' opinions about service provides, among other things. All of these, along with basic recommendations and expressions of trust, can be represented in the form of digitally signed documents, i.e., certificates.

In order to be useful, the handling of these kinds of trust expressions should be integrated to the trusted computing base (TCB) of the used computing system. That is, the security mechanisms of the underlying operating system should be extended to understand where, when, and for what purpose trust is needed when conducting transactions over the network. In practice, this means that the operating system takes responsibility for securing the network connections, and whenever running an authentication protocol in order to open a new connection, takes care of evaluating the trust requirements of the requesting application, together with the credentials of the server and client programs. In [P3] it was described, how this could be realised multi-user operating system running TCP/IP protocol stack and using the IPsec security protocols. The security policy would be based on the trust expressions the user has stated earlier, augmented with online user interaction when needed. On opened connections, the trust assumptions and credentials were suggested to be separately bound to each IPsec security association (SA), allowing SA sharing whenever the needs of a new connection match with ones provided by an existing SA (Nikander 1999). As another example, we considered how Java/Jini based ad hoc communities could be secured with SPKI certificates, and how simple application specific trust relationships could be represented in that kind of information (Eronen et al 2000).

Bertino et al approach the issues from the knowledge management point-of-view, with a good presentation of the overall state of work in this area (Bertino et al 2006). They present the *trust negotiation* (TN) approach, which is exploiting the concept of properties of the entities as a means for establishing trust, particularly in open environments such as the web, where interacting entities are usually unknown to each other. TN is a P2P interaction, and consists of the iterative disclosure of digital credentials, representing statements certified by given entities, for verifying properties of their holders in order to establish mutual trust. In such an approach, access to resources (data and/or services) is possible only after a successful TN is completed. A TN system typically exploits digital identity information for the purpose of providing a fine-grained access control to protected resources. However, unlike conventional access-control models, TN assumes that the interacting parties are *peers* and that each peer needs to be adequately protected. For instance, with respect to the peer owning the resource to be accessed, assets that need to protected are, in addition to the resource, the *access-control policies*, as they may contain sensitive information, and the *credentials* of the resource owner. With respect to the peer requiring access to the resource, the assets to be protected are the credentials as they often contain private information about the individual on behalf of whom the peer is negotiating (Bertino et al 2006). How to communicate the relative success of failure of the TN to the user, and finding out what else the peer might consider private, and how to show that the privacy is being preserved, are some examples of the "human problems" in the TN approach.

These are by no means the only solutions, but they represent different approaches to the problem. One area still requiring considerably more study is the relationship of these kinds of security measures, enforced by the operating system, and the user interface. It seems that something similar to the trusted path is needed. Other related areas include database seucrity, security for GIS (Geographic Information System) data, an increasingly important area for national security, for information-grid architectures and for sensor data as well as privacy and security for Web services and the semantic Web (Bertino and Sandhu 2005).

To be able to bring together the different worlds of technical trust and real-world trust expressed by users, we should look for a mechanism that will

- express trust in a digital form and
- write a policy that uses this digital expression of trust
- in such a way that is technically secure and understandable by the users.

The key question is how to deal with the complexity that security inevitably holds within. Decisions about security, or trust, are not by their nature simple. How could we guarantee that users could, at the same time, make a simple yet accurate decision about trust? Will existing technical solutions be appropriate enough to provide means to map these novel user needs, or should we, after finding out the real user needs try to build something completely new? Furthermore, would this be based on some kind of a general model of trust, or are we more likely to experience a multitude of application specific trust management systems?

From the user's point of view, the problem areas include the following:

- How to separate trustworthy and untrustworthy services from each other?
- How can a service provider let users know that it is trustworthy?
- How can users get information about security and trust issues in a form that is understandable to them? What kind of information do they need and want?
- How can users manage their security needs in a way that is both usable and meaningful?
- How can we motivate the users to care about their security in a positive way, and not to consider it as a burden?

On the other hand, even if the human can in fact be pointed out as the 'weakest link', also the computer systems are not infallible. Diomidis D. Spinellis gives a nice handling to this well-known dilemma. According to him, even if some users, especially the 'average man' often treats computers as 'godlike' and this also reflects the current refrain of computers as the most ingenious invention of the king of the creation, the humans, we are, in the end, aware that the system we like to see as omnipotent can ultimately fail: The system is breakable (Spinellis 2003). Spinellis also uses the metaphor of the 'weakest link'. According to him, it will not be enough that the apparatus is secure and its operation system a closed one; also the programs that it is running need to be complete and carefully written security-wise. For the security of computer security to actually happen, Spinellis states that the current systems tend to become too large, complex, and elaborate to run to be effective and usable. A central solution in this area is an unlikely solution according to Spinellis.

This issue is related to the often poorly handled difference between *trustworthiness* and being *trusted*, according to Ross Anderson (Anderson 2003). Anderson claims that trustworthiness is a stronger term: it denotes the idea of being unbreakable. The trust provided by this system will not be broken. Instead, *trusted* can mean almost anything – anyone can decide to trust anything on any grounds. The term trusted only states that trust is taking place. This fundamental difference between the two terms and their meaning must be kept in mind when researching the contents of trust situation currently under investigation, and trustworthiness of, say, an online situation, should not be falsely promoted among trusting users, if there really are not good grounds to do so. The alleged trustworthiness or untrustworthiness of any online service must be clearly and unanimously visible to the user, who must be able to make correct decision about whether it is wise to trust or distrust the service or system at hand.

4.1.1 On privacy

Trust is closely related, and in fact intertwined with the notion of privacy, and sometimes it is hard to tell the two apart – they are clearly interdependent. In practical research, however, there exist two separate lines of research, one on privacy, and one on trust. This is why the topic of privacy is only shortly touched on here, and to limit the scope of study covered. However, in any treatise on trust, something must be said about privacy as well. Let us concentrate on *privacy online.*

Considering an online service trustworthy means, among other things, considering the information provided for the service and all the conducted transactions to remain private (e.g. Anderson 2001). This, then, means that the information will not be available to others, and will not be used out of context, for example. Privacy is indeed one of the top priorities of consumers intending to use Internet-based services, and it seems to be ahead of such qualities as ease-of-use or cost (e.g. BusinessWeek/Harris Poll (1998) and (2000)). The use of Internet is threatening consumer privacy in new and extreme ways, and people are willing to take the time and effort to make sure that their privacy on the Net is being protected (Hoffman et.al.1999). In a constant disappointment with the continuing current privacy-violating practices of the actors of the online environment, the voice of the general public tries to be heard via public interest activities such as Electronic Privacy Information Center, EPIC (www.epic.org). EPIC is a public interest research centre based in Washington, D.C. It was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values. EPIC has published annual and several separate reports on the current (poor) state of privacy online (e.g. EPIC 2005). **Figure 1** presents a list of some of the demands for ensuring privacy presented by the organisation.

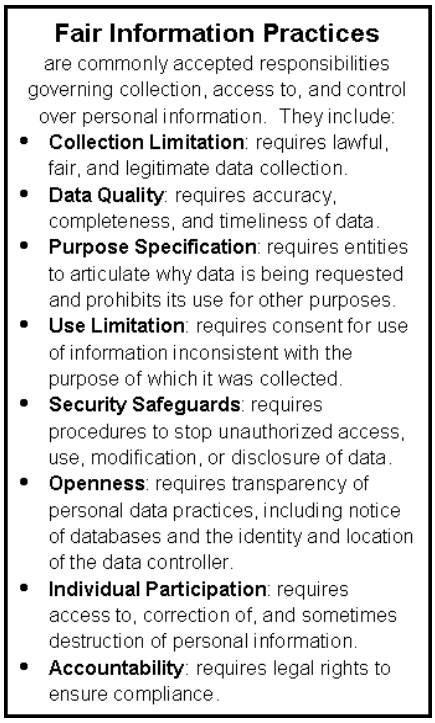


Figure 1. Epic's list of fair information practices. (Epic 2005)

In order to protect users' privacy, we need to know its scope and limits. But defining privacy is not an easy task. Privacy is a basic human requirement we have a fundamental right to, but this does not reduce its ambiguity. What is regarded as private varies across organisations,

cultures and even individuals (Adams and Sasse 1999b). Another look in a Thesaurus tells us that privacy is "the quality or state of being apart from company or observation, that is, seclusion" (1 a), or "freedom from unauthorised intrusion, one's right to privacy" (1 b). In the archaic sense, privacy can also mean "a place of seclusion" (2). The third and last meaning given us by the Thesaurus links privacy with security through secrecy, depicting privacy as "secrecy" (3 a), or as "a private matter, secret" (3 b). A traditional way to look at privacy is to focus on the defensive role privacy can play in limiting others from access: either from access to oneself or to information about oneself (Taviani 1996).

If we concentrate on the case of online transactions, we can state that privacy includes both the privacy of personal information supplied by the user for the service-provider as well as privacy of any transactions (that involve the use of money) performed by the user online in the Internet. In a study done at AT&T Labs-Research (Cranor et al 1999), a questionnaire on users' attitudes about online privacy, it was found that the general attitudes of the users varied greatly, when it came to the question of what is considered to be private. The users were loosely grouped into three categories in their attitudes towards privacy. These were:

- The **privacy fundamentalists**, who were extremely concerned about their privacy,
- The **pragmatists**, who were also concerned about their privacy but were ready to trust the services if there was some sign of existing privacy protection, and
- The **marginally concerned**, who were willing to give data to web sites under almost any conditions.

The implications of this study suggest that one of the major issues in implementing any privacy protocols will be designing suitable UIs for them. On basis of the analysis of the completed questionnaires the researchers were able to draw some general guidelines for the design of secure UIs:

- such systems must inform the user when privacy might be at risk and
- this must be accomplished in a seamless and unobtrusive way
- very simple interfaces are likely to be useful and usable for both users with strong feelings about privacy and users with very little concerns about privacy issues. However, the "pragmatists" may need a different approach in UI design best suited for them.

Among the most important findings was the conclusion that it seemed unlikely that there could be a "one-size-fits-all" approach to online privacy that would be successful. The users were too heterogeneous a group in their opinions, assumptions and the amount of appropriate knowledge for this to be possible. It is also likely that there will be not just individual differences but also cultural ones what comes to the makings of privacy: The need for privacy and the requirements for experiencing when the standards for privacy are being met is likely to vary culturally as well.

The part privacy plays in trust can be demonstrated via the analysis by Good and Krekelberg on the usability of KaZaA file sharing application (Good and Krekelberg 2003). The work is based on (Whitten 1999) and deals with the usability issues in file-sharing over network. Even the topic of the paper is not really trust, from this work can nicely be used to show how privacy of the user can be shattered by bad usability, leading to the disappearance of trust the user was originally feeling toward the system. In the case of using KaZaA, trust is primarily lost due to the fact that the *control* is taken away from user, who has little means to gain understanding on what consequences the choices have on the level of sharing.

KaZaA is primarily intended for sharing multimedia files across users via network, but it can also be used for sharing other types of data between the users. One objective of the research

was to investigate, how understandable are the current file-sharing procedures of KaZaA. The researchers had noticed that it is likely that users end up sharing more files than they have intended. In addition, they were likely accidentally to share information that was private in nature and that they did not really wish to share. KaZaA represents a model example of an application that was originally intended only to be used by experts, but which has later been spread to a much wider and more heterogeneous user base. This is a typical background in area of trust, and explains to some extent why the usability problems can be so huge. Maybe the biggest problem is that users are treated as if they were experienced network administrators, giving them rights to conduct changes the consequences of which they have no way to understand, nor handle. In KaZaA, for example, it is possible share user's Inbox or personal diary with the rest of the network, without user even noticing that this has happened.

Giving too much rights, and too little information is a dangerous combination only too typical. In practice, the security of the system used has been made the responsibility of the non-suspecting user. The outcome of this setting often is that user is compromising his security without knowing. A basic requirement in good usability in the area of security is that such mistakes should not be possible, and the responsibility is not left to the user alone. The system should be 'wiser' than the user, preventing dangerous errors from the user (e.g. Riegelsberger 2003, Adams and Sasse 1999). Motivation for caring about privacy can also be provided by personalised privacy tools that enhance trust; at present, a user with particular privacy needs and policy often lacks the means to fulfil them (Lau et. al. 1999), (Rocco 1998), (Ackerman et al 2005). Users interested in their privacy often have to also conclude that the privacy information on most sites is confusing, incomplete, and inconsistent (Surfer Beware III 1999), (Yee 2005), even if the users would show an interest towards this kind of information. Privacy has also often been balanced against other, competing interests, both personal and others' (Clarke 1999), (Yee 2005), (Ackerman et al 2005).

However, studying privacy more in depth is well covered elsewhere (e.g. Wang et.al 1998, Pedersen 1997, Kelvin 1973, Adams and Sasse 1999, Clarke 1999, Camp 2003, Camp&Osorio 2003, Ackerman et al 2005, Yee 2005, Cranor et al 2006; see also the P3P project (www.w3.org/P3P/)), and falls out of the scope of this study. However, it should be kept in mind that when trying to come up with trust-enhancing solutions and an understanding of trust, there also has to an understanding on the privacy issues at hand as well. Furthermore, on the UI level, many of the same principles may apply when dealing with either privacy or trust. Trust and privacy can, in a way, be described as two sides of the coin - inseparable elements in online transactions, varying, for the most, only in the viewpoint selected.

4.1.2 Definition of trust

What all these approaches towards trust do seem to have in common is the belief that introducing trust into the situation means that there is incomplete knowledge (parties involved do not know everything about the situation), and trusting behaviour means taking a risk: the trusting party becomes vulnerable to harm by the other party. Without such risk and without incomplete knowledge, trust is not needed. Further, in order to be willing to take such a risk, the trusting party has positive expectations about the good will of the other party (Friedman 2000, Olson and Olson 2000). This forms the basic formulation for trust for our purposes here:

> **with trust we mean succumbing into risky interaction with another party, with positive expectations about the goodwill of that other party.**

The goal of the technology designers (and us) is to inspire such trusting behaviour through igniting a cognitive state of trust in the users through the design that will, consequently, lead

to a smooth human-computer interaction due to trusting behaviour (Cassell and Bickmore 2000, Shneiderman 2000). Futhermore, for simplicity's sake, we use the words “trusted” and “trustworthy” in an interchangeable manner, since from the user's perspective, these two terms fall in the behavioural level into the same category. For the user, any system that is considered trustworthy, is also trusted.

4.2 Capturing human trust

In previous studies, there have been many different approaches to the problem of forming trust. In July 1998 the U.S. Federal Trade Commission Chairman Robert Pitofsky suggested a model with four basic practices regarding the use and gathering of personal information about the users (Privacy Online 1998):

- Sites should provide the user with information about their information collecting practices along with how they use the gathered information;
- Sites should offer the user the possibility to choose how this information can be used for these other purposes;
- Sites should offer the user access to gathered information with the opportunity to correct any inaccuracies and
- Sites should strive to protect the security and integrity of that information.

To guarantee that sites act according to such recommendations, imposing laws on online behaviour is an approach that seems to be favoured by the users, which is quite natural, but which in itself is not likely to be sufficient. Online trust depends on many factors, including consumer rights, freedom of expression, and social equity (Clarke 1999). Trusting an online service provided by a well-known bank is to a great extent based on users’ knowledge (or assumptions) about the laws binding all the business operations of the bank. In most studies about computer security – including ours – the users report on finding legislative intervention by the state desirable and necessary for promoting online trust (e.g. [P2], Hoffman et. al. 1999). Furthermore, behind this trust in the legality of the bank is, to put it bluntly, the sub-conscious trust in the basic structures of the society to remain stable, the trust in the status-quo instead of anarchy — in short, the trust and belief in the good-doing nature of a social contract between men, in the Rousseau*ish* sense (Rousseau 1762/1987).

Another kind of “social contract” is suggested to be executed in the cooperative relationships built on the Net: According to the study by Hoffman et. al. (1999), over 72% of Web users would have been willing to provide the service provider with personal information if only the sites would provide the customers with a statement about how this information would be used. Still, it seems that users do not consider information about themselves as merchandise, to be sold to the highest-bidding offer: in the Hoffman et. al. Study (1999), most users were found not to be interested in selling their personal information. What is noteworthy in all this is that having legislation over the matter may not be enough, if users do not understand how the current laws should be applied in each situation. Further, having such legislation may be misleading, as legislation has trouble in following the technology developing at a high-speed accurately. Administration officials fear that regulation may not keep up with emerging technologies, and it is not a good idea to have existing regulation of legislation that cannot be enforced. In fact, it may give people wrong assurances about assumed security. Also, the existence of a specific law may make people think that things have been taken care of also security-wise, even if this might not be the case ([P2], Litman 2000). Legislation alone cannot be the answer to trustworthiness – other means are also needed.

4.2.1 The Ecommerce Trust Study

The most comprehensive study on trust as regards the Internet in the beginning of our studies that we know of was the Ecommerce Trust Study committed as a joint research project by Cheskin Research and Studio Archetype/Sapient in January 1999 (Cheskin 1999). The study was made to find out about the nature of elements behind communicating trust to the user in ecommerce sites, both transactional and graphical. This research study was undertaken to determine the nature of those elements that communicate "trust" in ecommerce sites, be they transactional or graphical. The research objectives included the following:

- Obtain consumer and expert feedback in order to identify the elements that communicate trust
- Develop a "model of the building blocks of trust" based on that feedback;
- Map the relative importance of the most fundamental components that communicate trustworthiness as a guide for builders of sites;
- Learn more about the "state of the art" of Web site design; and
- Explore a range of additional issues related to consumer perspectives on trust and ecommerce.

The methodology in this study included 4 phases:

1. Consumer questionnaires analysed to develop model of Internet trust
2. 60 ecommerce sites audited on aspects of trust
3. Expert discussion to refine model
4. Consumer rankings of 8 sites that differed on the dimensions of fulfilment, brand and navigation

It is to be noted that all questioning and discussion was conducted virtually, through web questionnaires and virtual chat-spaces, not face-to-face.

The researchers came up with six fundamental forms to communicate trustworthiness online, as well as with a general understanding of the "state of the art" of the current situation in Web design as regards the issue of forming trust in the Web. According to this study, the six primary components to communicate ecommerce trust were considered the following:

1. seals of approval – symbols, like VeriSign or Visa, to assure the visitor that security has been established
2. brand – well-known brands are successful inside and outside Web
3. navigation – the ease of finding what the visitor seeks
4. fulfilment – information on how things will proceed and where to seek help if something goes wrong
5. presentation – high-quality design that connotes quality and professionalism
6. technology – high technology features connote professionalism, even if they are difficult to use

According to the outcome of this study, to start trusting is slow: trust is formed gradually, it takes quite a lot of time and repeated good experiences. Online trust can be described in terms of a human relationship. The initial stage is that of interest and suspicion; there has to be a motivation, a need, to become interested in the service, but this curiosity is stamped with distrust and suspicious caution in the beginning of the usage of a new online service. Thus, according to this study, trust is formed slowly as a function of time, and the feeling of control forms the basis for trust. Navigation was found to be key to meeting user needs and was a pre-condition to trust (which was a pre-condition to sales).

So, trust may, according to this study, best be described as a dynamic phenomenon, or as a process that starts with initial "indications" or "hints" – manner, professionalism, and sensitivity, for example – that enhance trust, and then slowly develops into "character traits" that receive an emotional response from the user. At this point the trustworthiness is best described through the concepts of dependability, reliability, and honesty. The behaviour towards the service is rather informal now, and the trustworthiness is not questioned anymore, at least not frequently. The user feels she has control over the situation, and over information about herself (Ecommerce Trust Study 1999).

Our first user study took place before we became acquainted with the Ecommerce Trust study. It is, thus, of great interest that the outline and results of the two studies would prove to be very much alike, thus corroborating one another and adding to the credibility of both studies. There is, however, a major difference across the current study and all the above-mentioned user studies: most other studies that exist have used polls in form of questionnaires as their primary source of data. It was felt that there is need for a study with emphasis on qualitative user interviews. This was the part of the motivation for the choice of methodology for the studies presented here.

The ecommerce trust study was repeated by Cheskin the following year, with some modifications (Cheskin 2000). This time the study concentrated more on differences between Northern and Latin American users, and indeed some variations in attitudes were detected. However, this work represents for the most only affirmative information on the results of the first study, and does not represent a novelty in its research design, so it is not dealt with in detail here.

4.2.2 The Untrustworthiness of the Web

Interest on the topic of online trust has also been expressed by Jacob Nielsen, a renowned usability guru, who has described the current state of the Web as one of untrustworthiness, where "customers are traded like sheep", and has also conducted his own studies on trust that confirm this (Nielsen 1999a, further elaboration on Nielsen Norman 2001) (This statement has been further confirmed by other user studies, e.g., (Hoffman et al 1999)). In practice, this means that e-business has not taken the customers' need for security into any consideration at all. According to Nielsen, this has to change, however, if one wants to establish any decent business on the Net, and other researchers strongly agree. *A climate of trust* (Nielsen 1999a, see also Rosenbloom 2000, [P3]) must be promoted whenever there is a need to create a functioning network in a virtual world, and that is what the electronic marketplace essentially is. Mutual trust is always needed for good-quality relationships, be they between two people, a group of people, or between a user and an online service. Trust is formed through experience, it is a long-term proposition – that is, it is hard to build and easy to lose (Nielsen 1999a).

Nielsen states that on a Web page, trustworthiness can be communicated through use of seals of approval, brand reputation, appropriate use of technology, and through design in the following way (Nielsen 1999a):

- **Design quality**: professional appearance feels solid; clear navigation conveys respect for customers and an implied promise of good service. Typos or difficult navigation communicate disregard for the users.
- **Up-front disclosure** of all aspects of the customer relationship. For example, shipping charges should be revealed immediately rather than waiting until after the user has placed an order. A few people may be cheated into ordering by hiding the shipping costs, but many more will abandon the site at an early stage of the process.

And those users who do get cheated will most likely be angry at being cheated, and will not become regular customers.

- **Comprehensive, correct, and current** content and product selection feel solid. If a site has product photos, it should have good shots of *all* products. Haphazard, random content signal a brittle service – the web pages and the photos on them should be updated at the same rate as the products or services themselves are updated, not later.
- **Connected to the rest of the Web** with links in and out. Not being afraid to link to other sites is a sign of confidence, and third-party sites are much more credible than anything you can say yourself. Isolated sites may feel like they have something to hide.

Clearly, Nielsen's recommendations are a good start for creating trustworthy design, and most of his suggestions are easy to follow. However, the notion of *design quality* remains somewhat unclear: what is meant with "professional appearance"? Unfortunately, Nielsen does not provide any further clarification of this notion. However, he goes on by declaring that users must be given a feeling of being in control and knowing what is happening. The notion of *being in control* has also come up as a major ingredient in promoting trust in other studies about users and trust as we have seen, e.g. (Cheskin 1999) presented above. Other such guidelines for inducing trust have also been presented (e.g. Friedman 2000, Olson and Olson 2000), but the contents of these is more or less the same as those presented in the (Cheskin 1999) and also by Nielsen (1999a).

4.2.3 Credibility or trust? – the work of B.J. Fogg et al at Stanford

At Stanford, B.J. Fogg has been conducting trust research based mostly on online questionnaires, but also user evaluations, for several years[2]. Interestingly, also Finns were included in their online query in 1999 in an online version of a local tabloid, where users' bases of trust were investigated, providing a good basis for comparison with the user studies that form the corpus of this thesis, as well as with those conducted by Jarvenpaa and Tractinsky et al (1997, 1999). The Stanford research group has published actively in major forums and journals of HCI field, thus having quite a lot of impact on how trust is perceived in this field of research. A good summary of this work can be found in Fogg's book on Persuasive Technology, were not less than 50 pages, in two separate chapters, have been dedicated to handling trust (Fogg 2003).

Fogg prefers the term 'credibility' over trust, defining credibility as consisting of trustworthiness and expertise. Trustworthiness is defined as truthful, fair, and unbiased. Further, perceived similarity is seen as key ingredient in making something appear trustworthy. Expertise, on the other hand, is made up of perceived knowledge, skill, and experience of the source, judged against several cues, such as titles, labels, appearance cues, etc. Fogg emphasises the role of perception, talking about *perceived* trustworthiness and *perceived* expertise making up *perceived* credibility. This choice of terminology is justified by Fogg by stating that the term trust seems too vague. Fogg handles trust as part of this book because he sees trust as a central factor in persuasiveness[3].Fogg deifnes, presents, and analyses various types of human-comuter interaction situations, where he believes credibility plays a crucial role. According to Fogg, credibility matters when computers

1. instruct of advise users
2. report measurements
3. provide information and analysis
4. report on work performed
5. report about their own state

[2] http://captology.stanford.edu/
[3] The main topic of this book is persuasiveness – how computer technology can change people's behaviour and attitudes.

6. run simulations
7. render virtual environments.

On top of this, Fogg has built a novel kind of usability taxonomy. He sees credibility as consisting of four different types of credibility. These are:

Type of credibility	*Basis for believability*
Presumed	General assumptions in the mind of the perceiver
Surface	Simple inspection or initial firsthand experience
Reputed	Third-party endorsements, reports, or referrals
Earned	Firsthand experience that extends over time

Table 1. Credibility according to Fogg (2003).

Fogg claims that dividing credibility in this way presents novel information. In a way, this is true. However, the novelty is mainly based on the fact that Fogg is using the term ’credibility’ instead of ’trust’. If we, again, swap the terms, there is hardly anything new in this analysis. Already in (Cheskin 1999) these different types and levels of trust are presented, so are the effects passing time and personal experience have on how trust is developed.

The different credibility types can appear jointly or separately, and usually credibility is built up some kind of mixture of several credibility types according to Fogg. It would be interesting to try to find out, if and how various trust-demanding situations could be grouped according to the credibility type(s) they require. If successful, such analysis might be helpful in designing trusted services.

Surface credibility, dealing with e.g. how the visual layout of a web service affects the credibility of that service, is interesting from the point of the discovered importance of online aesthetics to trust formation (e.g. Tractinsky 1997, Tractinsky et al 2000, [P7], Lavie et al 2004, Lindgaard et al 2006, Cyr et al 2006). Many have tried to present design principles for trusted design (such as Cheskin 1999, Nielsen 1999, Egger 2001, 2003, Cyr et al 2006). The recent empirical studies by both (Riegelsberger 2003) and (Lindgaard et al 2006), as well as the ongoing cultural study by (Cyr et al 2006) have corroborated the hypothesis about the significance of decision-making about trustworthiness on basis of aesthetic factors. This is especially the case, when other factors of credibility, such as e.g. reputation, do not apply (Lindgaard et al 2006). However, Fogg does not really elaborate on this topic, stating only that surface credibility plays an important role in trust-promotion, with a brief analysis of the ingredients of the affecting design. According to Fogg, these are: aesthetic pleasantness, fulfilment of positive expectations, and signs of importance, or power. Fogg also states that the ’design kit’ or formula for trust-inducing design still awaits its discoverer.

Over 6000 respondents have participated in answering the questionnaires at Stanford. The study has been repeated every 2-3 years, with updates. Fogg is also planning to continue repeating the study, thus providing a longitudinal type of data on the development of user attitudes about credibility (trust) over time. A main benefit of quantifiable research that the questionnaires represent is that it enables such massive samples from the user base and the creation of trust information database.

However, it is a good question whether the chosen line of study will prove best results in studying such an issue as trust fundamentally is. Trust is for a big part implicit and emotional, and starts building up on an unconscious level (e.g. Cheskin 1999, Lindgaard et al 2006, Camp 2003, [P1], [P7]). Users can in general not always report their own actions in a reliable manner even when dealing with simple, concrete issues such as reporting their morning activities (Norman 1986) – with trust issues, this is likely to be even less the case. In addition, advance evaluation of future actions is often quite difficult to users [P1]. Using preset

questionnaires and fixed-time phone interviews, can effectively stop the possibility for probing for getting deeper into the reasons behind the alleged answers.

To give an example of the restrictions of this research line: in (Fogg et al 2003) is presented a credibility study where 10 different types of online services were analysed by 2684 users on basis of their perceived credibility. The most trust-inducing factors were visual design, information design, and information-centredness. But what do these concepts actually mean? The interpretation of such issues by ordinary users is a challenging task, and misinterpretations can lead to serious deviations in the validity of the gathered data and its analysis. Even though user evaluations are used, their gain is disputable if the terminology used is ambiguous, and especially if the answers of the respondents are not probed any deeper into. In the case of visual design, even graphic design professionals cannot agree on its meaning to an agreeable level, as (Lindgaard et al 2006) have shown. Since trained graphic designers are more likely to share common understanding on the ingredients of the visual design on basis of receiving similar type of training, it is likely that if their opinions on these factors shows such strong deviation, this will be amplified among the 'average' users and their opinions. Luckily, also Fogg admits to the vaguenss of the categories used.

The topics of research Fogg has selected are quite interesting and one would expect more from the results. However, they do not succeed in going beyond surface level, even if also UI evaluations of existing services were also used as a method. This may be due to not only the selected methods but also to the fact that it is very challenging to study via *any* methods – many have tried it, sometimes with poor results despite major efforts. It seems that combining various research tactics is likely to bring the best results in trust research: a mixture of qualitative and quantitative techniques will probably be best. The Ecommerce trust study (Cheskin 1999) was an early, good example of such research design, user evaluations with expert analysis, and more.

4.2.4 Consumer Trust: Consumer WebWatch Web Credibility Project

Princeton Survey Research Associates (www.psra.com, PSRA) has gained wide publicity on their trust study in 2002 and repeated in 2005. This study bears some similarity to the Ecommerce Trust Study by (Cheskin 1999, 2000) discussed earlier. Consumer Reports WebWatch, who ordered these studies from PSRA, is a independent, non-commercial organisation that opearates on the customer interests (http://www.consumerwebwatch.org).

The study is a national study, conducted in the U.S. via phone interviews based on a questionnaire. In all, 1501 Internet users were interviewed about various areas about their Internet usage.

The results of the 2005 study indicate that trust had diminished from that of 2002

- Nine out of ten U.S. citizens over 18 Internet users had changed their online behaviour in order to protect their identity in the fear of identity theft.
- Of these changes, 30% involves less overall usage of the Internet.
- 25% had stopped making any online shopping.
- Of those still conducting online shopping, 29% was buing less frequently online.

As major threats was seen identity theft as well as losing money to malicious actors. Online merchants were trusted slightly more than auctioners. Online news services and news group were trusted as much in 2005 than in 2002. Instead, the information companies were providing about themselves was clearly distrusted.

Users had become more analytic about the basis for choosing a specific online merchant over its competitors by 2005:

- 88% considered the privacy of personal informantion very important
- 81% considered the trustworthiness of information to be very important (up by 1%)
- 76% considered the visibility of sources of presented information very important (up by 8%)
- 73% considered the timeliness of the information and frequent updates very important (up by 8%)
- 48% considered the visibility of ownership very important (up by 16%)

Internet was rather well trusted as an information provider. Users had, however, become more critical in 2005, and were expecting the following factors from news services in order to trust them:

- 69% wanted to see a clear difference between advertisements and the news (up by 10%)
- Users wanted to be able to identiy the face behing the news; also a feedback channel was found to be important. 47% considered showing the editor's email address very important (up by 11%)
- 44% found it very important that the news service would publish corrections and clarifications to previous news in a central place. (up by 10%)
- 31% considered very important that the financial ties of the publisher of the news service were clearly announced (up by 9%)

Unfortunately, from the study it cannot be really deduced what the users base their judgements on. For example considering that one's privacy is being preserved is not straight-forward but can be ambiguous. It would be interesting to try to find out, what kind of privacy criteria the users could identify as basis for these judgements. The same is true about judging the trustworthiness of information which in this study seems to be more or less based on the visibility of the author identity and having a feedback channel, preferably directly to the authors or editors themselves.

It is interesting that according to the study it takes more trust to conduct banking online than is needed for online shopping. According to the outcomes of the user studies that form the basis for this thesis, in Finland users were quite trusting towards online banking already in 1999, when all other online shopping was still considered quite untrustworthy and few were doing it. [P1] One reason behind this was that in Finland there exists a great amount of trust towards the banks. In the studies it was found out that this trust was based to a great extent on the fact that the operations of the banks are tightly governed by laws. Further basis for trust towards the banks was that users felt that banks had to be able to be trustworthy online, since if they failed this, the users would lose their trust toward their bank altogether and take all their business to another bank. In other words, the users were thinking that for these reasons the banks were forced into securing their online services to the level of truly being worthy of their trust. In a way these views were so strong that the attitudes of the users were almost reaching the situation where they felt they did not need any trust towards the banks at all, since there was in fact no risk – a leap of faith would not be needed. Instead, the expertise of online vendors in taking care of the security of the transactions was not trusted, and the users felt that here, trust would be needed but that trust did not exist. In any case, the U.S. users were more trusting towards the online banks than towards the online vendors – same as in Finland.

Also of interest in the study is that the most active online users were very trusting towards the services they used the most. If services were trusted only a little, they were actually not used. This is in line with the outcomes of the Ecommerce Trust Study: once a certain level of trust is needed, the trustworthiness of the service is no longer questioned, in order to ease the decision-making process. The reasons behind this also involve the need for humans to rationalize their behaviour and believe in the validity of their own decision-making. Once the usage of a service has been initiated on basis of some initial trust, this decision is no longer repeated but the decision is 'once-and-for-all' unless something bad happens (Cheskin 1999). This is a nice showcase on how the existence of trust simplifies the practical life and vice versa: the absence of trust makes life more complicated (Fukuyama 1995).

In all, the study clearly shows that the current level of user demands for willingness to base trust on the Internet actors has grown. Since these demands are not yet met, the users are expressing less trust towards the Internet than before. This trust will not be recovered until the online vendors find ways to answer these needs, and online use will not be growing at the expected rate.

4.3 Frameworks for trust

A big part of the existing trust research has focused on attempts to clarify and formalise the concept of trust. As this is a complex concept that can be viewed in many different ways, depending on the current issue at hand and area of study. In order to succeed in understanding trust and in building usable trust management systems also technically, it has become a necessity to try to create consensus across these different approaches to trust about the contents of this multi-faceted concept. Recently, a bunch of studies have concentrated on exactly these issues.

4.3.1 The Work of L. Jean Camp

Professor L. Jean Camp, currently with Indiana University, has many publication on the area of trust, spanning over several years. She bases her concept of trust in the work of Niklas Luhmann (1979)

Camp states as her fundamental research question the possibly neutrality of trust, what comes to representing human values. She has examined this question in identity management, voting systems and in ecommerce. Her working hypothesis is "that an examination of trust assumptions in security systems illustrates embedded values, and in particular these assumptions become embedded through technical simplifying assumptions that create social complexity", as she states on her university homepages (www.ljean.com).

Camp's book on the trust and risk in Internet commerce (Camp 2000), was one among the first to investigate the social patterns of online contexts. Camp has also made research on digital identities (Camp 2004), providing a quite usable identity taxonomy that could be tested with real users. In (Camp 2003), she has also provided an accurate classification of various types of privacy. (Camp et al 2001) present early work on placing online trust in the right social context. This work has been continued till this day, and is currently expressed in the work for the design of NetTrust, a browser-based tool for managing online trust, which is based on the previous work and will also be usability tested before release (Camp 2006).

The work of Camp is quite interesting, because she brings together a thouroug understanding of both the economical, technical, and social issues involved in making trust management more human. Despite the original lack of actual user studies, the research approach of Camp comes very close to that of the author of this work, with the difference that in the work at

hand, the understanding of the economical side is not very strong, and relies completely on the work of others.

Camp's work is further analysed in connection with the following various subchapters, in relation to other work in this area.

4.3.2 Measuring trust

In their work for creating a secure knowledge management system, (Bertino and Sandhu 2005), find out that the need to define trust in a measurable way becomes evident. They state that the problem with current trust definitions is that all these definitions is that they provide a notion of trust for which establishing metrics and developing evaluation methodologies are quite difficult. They decide to build their definition on top of (Blaze et al 1996), according to whom, "Trust management problems include formulating security policies and security credentials, determining whether particular sets of credentials satisfy the relevant policies, and deferring trust to third parties". Such a definition of trust refers to security policies regulating accesses to resources and credentials that are required to satisfy such policies. TN thus refers to the process of credential exchanges that allows a party requiring a service or a resource from another party to provide the necessary credentials in order to obtain the service or the resource (Bertino and Sandhu 2005).

In the HCI side, David Gefen from Drexel University has published many articles where he has brought up the multidimensional nature of trust, in order to make the trust ingredients measurable. He has chosen this approach since he found the previous treatments too holistic and felt that it would probably be more fruitful to chop down the concept to its ingredients, and then evaluate their relative meaning to the formation of the overall trust. By means of statistical significance, he has tried to prove that this approach is valid.

Gefen divides overall trust into three factors. These are the actor's 1) *integrity* 2) *benevolence*, and 3) *ability*. In fact, these three factors are quite traditional factors of trust from the technical point of view (e.g. Ganesan 1994, Shneier 2000). The purpose of Gefen's research, then, is to demonstrate that these traditional ingredients of overall trust can be shown to be effective in such a way that can be measured with statistical methods. According to Gefen, trust can be examined by analysing its ingredients, but also on a general level, as a sum of these ingredients as overall trust, where the identified ingredients can play a role with varying weight depending on the situation at hand. The key point is that the individual weights each ingredient has on a given situation, could be measurable.

Even if Gefen's attempt to formalise the ingredients of trust into a measurable format is valid, its merits are disputable. Even though the weights of different trust factors could now be analysed, how exactly to apply this information for trusted design, for example, remains to be solved. Gefen has ended up with results according to which for example window shopping and shopping involving actual transactions (closure) vary in the weights that the individual factors have in the formation of the overall trust in these situations. This seems rather intuitive: also in our user studies it has clearly come up that the shopping intention differs from the actual shopping situation in the amount of trust needed, especially so in the actual paying situation, where there appear new criteria for the trustworthiness of the transaction [P1], [P4]. Also other consumer research confirms these findings. For example, Deloitte (http://www.deloitte.com) published in December 2005 a 'Christmas Survey', where it was found that shopping-wise, Internet is mainly used for three types of actions: 1) familiarising with product offering and shops available; 2) price comparison; and 3) actual purchases[4]. These three sides of shopping are clearly separate in amount of trust needed (see also

[4] http://www.deloitte.com/dtt/press_release/0,1014,sid%253D2834%2526cid%253D103623,00.html

Conclusions). This is precisely the same point Gefen (2002) has wanted to prove. Readiness to engage in a transaction demands more from that transaction than mere surfing, even when this surfing has a purpose and a goal. The outcome that the three ingredients of trust would gain different weighs in these three different situations seems only logical.

However, the impact of Gefen's research to understanding of trust seems relatively small. In a further article in the same research line, Gefen has identified three problems in trust research, trying to provide solutions to them (Gefen et al 2002).. These problems are 1) oversimplifying the concepts of trust and risk, 2) the unresolved nature of the relationship between trustworthiness and trust, and 3) the idiosyncratic nature of the relationship between trut and risk. This analysis seems, however, not to lead to any new conclusions. Also (Araujo and Araujo 2003) state in their excellent review on current trust research that these attempts to clarify the concept of trust have not led to any consensus about the scope and precise contents of this multi-faceted concept, so their offering remains disputable. Araujo and Araujo present a handbook type of an overview of reseach on the topic, listing, in a down-to-earth way, the current state of trust research, significance of analysing the risks, the special requirements of the making the actual transaction, and providing also a set of design guidelines for increasing the usability of security, together with an extended bibliography. However, connecting these analyses to the work of, e.g. (Bertino and Sandhu 2005) would be quite difficult, and it seems likely that these different types of research lines will continue having a hard time connecting.

This seems characteristic of the discussion at hand – it is philosophical by nature and it is unlikely that consensus would truly be reached. Further, such consensus may after all be unnecessary – as in the case of the concept of "good-enough security", also with trust it may be enough to reach a sufficient level of trust, characteristic of each situation. Also, the views presented recently cannot really claim novelty: already in 2000 appeared an excellent work by (Grandison and Sloman 2000) that lists most of the issues currently being 'discovered'. The paper, named *A Survey of Trust in Internet Applications*, states, among other things that chopping overall trust into smaller parts is not likely to be too useful, since most applications and solutions involve more than one factor. They also present a taxonomy of trust, categorizing various types of trust needs on basis of 1) access control to own, private resources, 2) assessing the trustworthiness of a service provider, 3) trust problems related to authentication (identifying the actors reliably and having the authorizations and rights they claim to have) and 4) delegating trust. The concept of trust they define as *"…the firm belief in the competence of an entity to act dependably, securely, and reliably within a specified context (assuming dependability covers reliability and timeliness)"*.

This paper not so often referred to has its main emphasis on the request for clarifying the concept of trust in such a way that it could be translated into formal logic in order to be able to run a formal analysis on the causal relations of trust and other factors. However, Grandison and Sloman also present many other ideas that only now are being recognized by other, such as need for design toolkit for creating, analysing and monitoring trust relations; observation on the need to define not only trust but also *distrust* – often neglected other side of the coin – and the possibility to express not only trust but also distrust; and suggestion to apply risk analysis from economics to trust analysis.

4.3.3 The Work of M.A. Sasse et al

Sasse is one of the authors in (Adams and Sasse 1999b), one of the 'classics' in the field of usability and security, and Sasse has made, with her group, a considerable contribution to this area in all. A generic framework of trust has been the goal of also the group by Sasse in London: either come up with the methodological foundations for how to study trust (Riegelsberger et al 2003), or providing critical analysis of current approaches, and

suggesting new ones to replace them, including a game theoretical approach (Riegelsberger et al 2005).

In the work of Sasse et al, Grounded theory methods of qualitative field research are used, where results are come up with through the method of inductive reasoning have emerged from the social sciences (Glaser and Strauss1967/1980, Endres-Niggemeyer 1999). In the grounded theories, the theory based on observations in the field makes an incremental growth based on the findings. While much empirical research starts with a set of hypotheses and tests these hypotheses against empirical data, grounded theories are developed incrementally from empirical observation. A candidate concept or proposition is discovered and integrated into the emergent theory. Concepts are re-arranged periodically, leading to the gradual emergence of higher-level concepts. As new knowledge arises it is integrated into the theory. The theory approaches validity as changes engendered by new data (Sasse, 1997; Endres-Niggemeyer 1999). This approach is then combined with a multitude of methods derived from standard HCI involving user observation and usability testing, experimental psychology, eye-movement tracking, and even game theory.

We have already presented much of Sasse's work in previous chapters of this work, e.g. on usability of security, users as the weakest link, in the area of privacy, so it will not be repeated here. Sasse et al have also made major efforts to improve password usability (e.g. Brostoff and Sasse 2000, 2003). Also, the work of Riegelsberger, who has worked under Sasse's guidance, will be dealt with later, when the various elements of trust are discussed. Quite recent work of Sasse's group is investigating the structure of recommender systems, searching ways to improve their usability (Bonhard et al 2006). In this paper, they are proposing to enhance the usefulness of recommender systems by including *more information* about recommenders to the system. The research is based on a laboratory online experiment with 100 participants simulating a movie recommender system to determine how familiarity of the recommender, profile similarity between decision-maker and recommender, and rating overlap with how a particular recommender influences the choices of decision-makers in such a context. While familiarity – a factor found earlier to promote readiness to trust others – in this experiment did not affect the participants' choices, Bonhard et al report that profile similarity and rating overlap had a significant influence. These results were suggested to be helpful in understanding the decision-making processes in an online context and form the basis for user-centred social recommender system design. According to the researcher, by enriching the user information of the recommender systems, the social context is re-embedded to the virtual environment, thus enabling better-based trust decisions.

The work of Sasse et al is closely related to the more technical trust research, where for example Yolum & Singh (2003), have, in the area of artificial intelligence, analysed the possibility of automation of trust expressions: how autonomous agents, operating independently in large, open, and distributed environments (such as the Internet), could find out about the relative trustworthiness – or untrustworthiness – of the other agents. The need to be able to automate expressions on such level clearly is a necessity – however, once again the problem of how to define trust arises.

Yolum & Singh bring *institutional trust* to the foreground. The initial trust in this type of situations is based on trust in a known authority. In real life such authorities are, for example, established institutions, in a distributed system the licensors of digital certificates. However, the problem in an open environment such as Internet is that there is no central authority that could automatically provide the initial trust to the actors of that environment. This means that the initial trust and authorization as a trusted party must be brought into the open system in some way or the other. The available options are *local* and *social* trust. Social trust means recommender systems, where the recommendations by others, preferably from verifiable sources, form the basis for trust. One way to do this is to build *referrals* from one service to another. Current P2P systems are built on such models, e.g. eBay. Even if the system has its

flaws, it seems to be working 'well enough' for users to be willing to use this type of systems. Local trust means simply that the user bases his trust on own first-hand experiences of the online actors. No separate authorization is needed in the latter case – the trust is based on user's own decision-making – the risk is also left to the user, which might not be very tempting to the users of these systems.

Yolum and Singh notice that the previous attempts to certify trust have been based either social or local trust described above. They propose a new model, where *both* types of trust are involved. In their suggestion, the agents are gathering information on each other's trustworthiness locally, but can also provide for referrals for other actors of the system. Involving both types will, according to the authors, lead to the capturing of two features about trust that is not possible for other systems built on one type of trust alone: 1) when small amounts of money are involved, users tend to be ready to trust also less well-known actors, whereas when the sums go up also the perceived (and real) risk is higher and more trust tends to be needed. Further, 2) the transfer of trust becomes possible: if a service-provided is experienced as trustworthy provided of one type of services, this trust is transferred to other types of services provided by the same service-provider. In other words, also in the interactions of autonomous agents trust is based on cumulative experiences of the past behaviour of the good and bad actors. This type of 'trust negotiations' between agents are currently one of the central research issues in the technical trust research.

Research on the significance of reciprocal referrals and links for trust promotion can be done from another perspective, too: Stewart and Zhang (2003) have analysed how hypertext links from one web service to another diminish or amplify the trust felt towards the linked services. Mutual links was one of the corner stones of trust already according to the (Cheskin 1999). According to Stewart and Zhang, the less well-known online actors will indeed benefit from linkage with a better-known service. Instead, the better-known service-providers should take care with their linking policies, since links to less known or even unknown services may lessen the trust felt towards the otherwise well-known service, if the users do not trust the linked services. Furthermore, links denoting a *partnership* between the linked services were found as more trust promoting than mere commercials. However, it was difficult for the users to judge which type of linkage they were dealing with.

In an earlier study, Stewart has shown that how users group various actors of the online environment had major effect on the trust transfer between the services forming the groups (Stewart 2003). Thus, links between services has indeed proved to be one of factors definitely affecting the formation of online trust, as was hypothesized on basis of previous work.

4.4 On the various elements of trust

The conditions of trust vary, and till now no clarity exists in how the various ingredients of trust contribute to the overall trust. Some of these ingredients have, however, been identified and can be further studied, even when their combinatory effects yet remain uncharted. We have seen the reciprocal linkage is one such ingredient; others include at least *usage of images, feeling of privacy, informativeness, and the understandability of information, visibility of information and system state*, etc.[5]. There are many candidates, and they may have co-dependencies. We will now have a look at the current state of research on some of these suggested trust ingredients.

4.4.1 Usage of images

[5] Good lists on these elements can be found e.g. in Cheskin 1999, Nielsen 1999, Araujo and Araujo 2003, or Basu et al 2003.

How using images in, say, a web service affects trust building is a topic that was identified as meaningful in (Cheskin 1999) and later taken up by (Riegelsberger et al 2003). Riegelsberger has explored how photos of people on web pages affect the trust felt towards the service. The starting point for the research was on understanding the mechanisms in marketing, where pictures of smiling, happy people had been used for a long time in advertisements in order to create positive feelings – and trust – in the audience towards the advertised product.

To verify these assumptions to hold also in the online environment, Riegelsberger et al designed a set of user studies to gain experimental results on the phenomenon. Riegelsberger used eye-tracking methods for finding out about the ingredients behind trust, in order to overcome the fact that trust reports by the users themselves can only be partial due to the nature of the trust formation. Riegelsberger showed users services with photographs of people in this study. As research hypothesis, on basis of results from previous trust research (e.g.. Fogg 2002, Olson et al 2002), and from advertising, explained earlier, about the trust-promoting effect of using pictures.

Even if the research in part confirmed the existing knowledge, the results were divided, showing that the trust-promoting effect of people's picture is not as straightforward as was formerly believed. They seem to make it more confusing for users to try to come up with an evaluation of the trustworthiness of the service, leading also to somewhat surprising results: the trustworthy, established online services seemed to lose some trust due to the effect of the pictures, whereas the untrustworthy ones were gaining on trust received. In other words, users were making wrong decisions about trustworthiness because of the pictures.

Adding pictures is categorized as adding a *surface cue* for trust formation. Such surface cues are commonplace in everyday life, where the expressions, gestures, tone of voice, and clothing of other people trigger trust or distrust in us towards the other people. Same applies for physical stores, where the general atmosphere, behaviour of the staff, etc, guide us towards a decision about their trustworthiness (see also Camp et al 2003). In the cyberspace, such cues can be presented via pictures, and also via seals of trust or links to others who are considered trustworthy, for example. The idea is that trust would be *infectious;* spreading from one actor to the other, if there is a link between the two actors. The trust association between the two actors, in the user's mind, may happen on an unconscious level, and consists of both a rational and emotional ingredient, according to Riegelsberger et al.

Furthermore, the pictures create confusion to trust decisions only on first-time viewing. On the following viewings, users ignore the pictures (see also Riegelsberger et al 2002). One reason for confusion seemed to be a mismatch between the style of the picture and the service: if the styles were different, users did not know what to think about it. This is reminiscent of using advertisements, where happy, smiling faces with otherwise suspicious-looking content may create a affective dissonance in the spectator.

The research was conducted by placing the users in a real situation involving a risk instead of just interviewing them or making them fill a questionnaire. This is very good, since "actions speak louder than words" also in usability work: as in any situation, people may say one thing and do something completely different. Further, Riegelsberger states that trust is difficult to study via interviews, since people have a need to see and present themselves as rational decision-makers, at least in the current Western society. This is very true, and this is why also in the user studies forming the basis for this work, care was taken to watch for this effect, and observing actual usage was added to the methodological toolbox, whenever possible. Using eye tracking is also an interesting method, although interpreting the massive amounts of data collected can be quite challenging.

Riegelsberger also tries to make use of economical decision-making theories for analysing trust decisions in situations where the risk involved is a financial one. Even though already

(Jarvenpaa et al 2000) can be seen as attempting such an analysis, integrating economical studies to the user studies of trust in novel ways would most probably be quite useful.

4.4.2 New types of trust certifiers

The need for some kind of intermediaries in order to create trust has been suggested by many. Sometimes this role of the intermediary is filled with a governmental office, legislation, new entrepreneurs such as TRUSTEe, as well as such traditional 'trust managers' as banks and insurance companies. On the other hand, the need for this trust has been sought to be minimised, by introducing stronger means of encryption, and data protection, firewalls, certificates, and so on. However, these types of certifiers have not been enough to make online transactions prosper, so new ideas are needed.

(Tang et al 2003) introduce an idea about *taking an insurance* against online threats. The idea is simple: since engaging in online businesses is insecure, there emerges a possibility for a new type of online vendor that can make money by acting as guarantor for these transactions. In short, the idea is to buy trust in a way. The idea seems feasible except for the fact that how can the guarantor actually guarantee the transactions?

According to Tang et al, insurances are needed for three types of trust:

- *Marketspace trust.* The trust that both seller and buyer must have in the marketspace where the transaction will occur.
- *Buyer's trust.* The trust that the buyer has that the goods will be delivered as agreed.
- *Seller's trust.* The trust that the seller has that he or she will be paid for the delivered goods.

The meaningfulness of the idea of such insurances was tested with users in Singapore and South Korea, via a questionnaire type inquiry (25 claims, 5-point Likert-scale). 35 businesses from Singapore and 38 from South Korea participated in the study. The questionnaire was answered in interaction with the researcher in order to ensure that the respondents would understand the claims in a correct way. More data was gathered via in-depth interviews in seven companies operating in either the insurance or technology field.

The outcome of the study is not very surprising. Users were at first rather enthusiastic about the possibility of taking an insurance against untrustworthy online actors. However, when they learned they would have to pay for it, the readiness to use money for such insurance was very low. This is a rather typical reaction towards computer security: users would rather get it for free, maybe because it does not seem to bring 'added value'. Rather than paying, users were more willing to either take their chances or withdraw from the transactions in all.

Tang et al claim that the unwillingness to pay is against the common policies of the Internet, where people expect everything to be free. The buying motives for online shopping also entail getting things cheaper and more conveniently than elsewhere – a new payment conflicts with these expectations. Further, with a new charge added to the cheaper price, the final price may come so close to the offline price that the motivation to conduct online shopping disappears altogether. Taking an insurance also brings extra troubles to the transaction, and in user's mind may be compared with, for example, the logistics in physically moving to the shop and back home. Since in normal stores the trust issues are not so pending, the added cost may lead the user, again, withdraw from online transactions.

(Chong et al 2003) analyse the trust chains in somewhat similar fashion. They present an analysis on factors promoting trust or distrust in the users of online auction such as eBay or Yahoo! Auction. Chong et al see the need to certify only 1) the trustworthiness of the vendor and 2) the trustworthiness of the mediary. The outcome of this study comes down to noticing the cultural differences between the American and Chinese users, participating in the study, on a very abstract level. According to Chont et al, the American individualists base more of their trust in explicit trust seals and on themselves, whereas the more communally oriented Chinese trust only people they know personally or their own first-hand experience.

(Salam et al 2003) suggest that not only the traditional institutions of trust of the physical world, but also well-established online actors with a well-earned, long-term positive reputation, such as Amazon or eBay, might be able to act as guarantors. P2P recommendations that these both online actors use have already been successful in creating trust in the user towards their services – even when according to Salam et al, users also express some suspicion and distrust towards such P2P recommendation systems.

Furthermore, since actions in the online environment require *more* trust cues than physical world, where there are many implicit trust cues (e.g. Camp 2004), and often the whole transaction process is completely visible to user, there might be a need for more than one type of trust provides, not just the guarantors, for enabling trust in the online environment. These could include 1) the actual guarantors, 2) advisors, e.g. state authorities, and as a new type, 3) established online entrepreneurs, such as Amazon (Salam et al 2003). (Bonhard et al 2006) have

4.4.3 Trust and risk

Discussion on the relation of trust and risk in the context of online environments was more or less initiated by (Camp 2000). In her book, she was laying the groundwork for considering the risks of the Internet business, identifying the avoidable hazards which were, in her view, likely to be found on the road towards realisation of the Internet commerce.

Starting an important research line, risk perception has since then become one of the focal points of trust research. Researchers from Cheskin have treated this issue in their contribution to the 2002 edition of The Human-Computer Interaction Handbook (Diller et al 2002). Trust is depicted as an enabler of interaction with society, along with legislation. The idea as such is not new (e.g. Fukuyama 1995), However, for trust research the classification of different types of risks embedded in trust decisions, is insightful.

According to the authors, when a person or corporation considers lowering the walls to act in the world, they have historically faced six types of risk, four of which often involve direct economic transactions:

1. financial (risk of losing money or paying too much);
2. functional (risk of receiving the wrong or a malfunctioning product);
3. social (risk of embarrassment); and
4. physical (risk that we might be physically harmed).

In addition, engaging with the world puts us at risk in two other ways:

5. emotional (risk that one might be emotionally hurt by an interaction); and
6. identity (risk that others may impersonate us for financial or other types of gain).

The goal of being able to trust, then, is *risk reduction*.

Defining different types of risk seems quite useful from trust research perspective. Parallel to the analysis of the multi-faceted nature of trust, a similar analysis to risk – an undeniable factor in trust-formation – is recommendable. Using the approach by Gefen (2000, 2002) reported earlier, the significance of the existence of some type of risk or their combination in a trust situation – a primary requirement for the need of trust in the first place – could undergo a similar analysis, where the sum effect of various types of risks could become calculable.

First, we would need to analyse, what types of risks appear in what type of situations. For example, when conducting online transactions as in online shopping, risks number (1), (2), possibly also (3), and (6) will be present. On the other hand, being active in newsgroups or chat rooms seems to denote the existence of the risks (3), (4), (5), and (6): using these services may not be socially acceptable for some people, and depending on their topic – meeting an online 'friend' may also realise the physical risk, if one is unlucky. If the purpose of being online is to find a life partner, the emotional risk grows. Also, identity theft (6) – for example, getting one's online nick name stolen for somebody else's use – is a serious risk in most situations. Understanding the type of risk we are dealing with in each situation and linking them with the ingredients of trust might make this part of the trust decision-making measurable. Further, on basis of this understanding, a designer of an online service might ultimately be able to help users notice the risks involved and act accordingly, thus leading to increased feeling of control of the service, and further to increased amount of trust towards that service. It remains to be seen, whether drawing such connections between all these ingredients is possible or worthwhile.

Salam et al (2003) provide an interesting handling on how risks are *perceived* in (Salam et al 2003). They start by listing as obstacles of online shopping the common distrust of consumers towards online shopping security and the unwillingness to take personal risk by engaging in the transactions, and the impossibility of building long-term customership between online vendors and users. What is novel in their work is setting risk aversion in centrefold. Salam et al also state that users have practically no means either to perceive or evaluate the risks in each situation in a realistic fashion.

The cure for better perception of risks that in effect would lead to trust enhanced towards the service, is offered using the traditional sources of trust *outside* the cyberworld for promoting trust. These include banks, insurance companies and other authorities, such as state offices. These traditional actors could find a new role as *guarantors* also in online transactions. On basis of user studies presented here (e.g. [P1]), this would probably work: these actors, if online also, are already trusted more by the users than other online actors. Users in [P1] were very trusting of their online banks, and would have hoped for all payments to be possible via a link to their online bank.

Another interesting remark by Salam et al is that when the financial (or other, such as desirability) incentive grows, users are more willing to engage in transactions they otherwise would consider too risky. This feature came up also in [P1] and [P4].. Salam et al interpret this as users *perceiving* the risk in such situation as smaller than it actually is; however, on basis of our user studies, it can be claimed that the users may be well aware of the risk, but if the product to be bought is much cheaper online or not available elsewhere yet quite desirable, users seem to be willing to give up on their normal 'trust level' – the risk is better *endured*, in hope of better gain. This could be formalised as a 'law' *where there exists a correlation between the threshold value of tolerable risk and the financial incentive.* The risk evaluations are not fixed but co-dependent with the possible gain: if the possible gain is perceived as greater than the possible negative effects of the risk realised and the damage it may cause, users are willing to take that risk. It would be interesting to be able to convert these risk evaluations computational somehow, in order to build a mathematical hypothesis on the co-dependence of risk evaluation and financial incentive.

4.5 Other related work

Some other related work on trust include (Friedman et al 2000, Shneiderman 2000) on bringing trust research to the awareness of wider audience; and for some novel recommendations on how to enhance trust (e.g. Friedman et al 2000, Olson and Olson 2000). The effect of different modalities on building trust has also become one of the topics of current trust research (see e.g. Rocco 1998, Jensen et al 2000). A lot of work is ongoing on accessibility issues (e.g. Cardoso et al 2002, Hwang et al 2002, Keates et al 2002), and the universal access issues should also be considered from the point of trust and trusting behaviour. Furthermore, it seems inevitable that some new legislation is also needed to guarantee common rules for all online transactions (see e.g. Litman 2000).

Trust has also been approached from the viewpoint of the credibility and preservability of information by Hart & Liu (2003). This research stems from the problems with archiving information: how can users be made to trust digital archives as replacements for the traditional means of archiving. Another new area where trust is crucial is healthcare gone digital. It goes without saying that the needs for trustworthiness and privacy as well as the integrity of the data, to name a few, are of utmost importance in this area (e.g. Luo & Najdawi 2004).

Also of interest is a study by Teltzrow et al (2003), where the effects of multi-channel delivery on the formation of trust were investigated: if an online vendor also has a physical presence as a 'normal' vendor, does this promote the trust towards this vendor? It appears, according to their study that their hypothesis on the positive effect to online trust of the physical presence, depending on the *physical size* of the vendor, was somewhat corroborated in the study. The work was built on the outcomes of (Jarvenpaa & Tractinsky 1999), according to which the perceived size and reputation have an effect on the trust felt towards the online vendor.

Easy-to-use authentication methods (Basu 2003, Frescha et al 2005), trusted design (Camp 2003), toolkits for promoting trust (Yang et al 2005, Wang et al 2005) etc will certainly be an important part of trust research also in the near future. In addition, the multi-disciplinary nature of trust studies is likely to expand: one example of this is introducing the theories from personal psychology to understanding, for example, different personality traits and their effect in making trust decisions online (Feng et al 2003, Saariluoma 2004).

Kim et al (2003), on the other hand, have concentrated on investigating the meaning of the feeling of satisfaction in consumer experience and the feeling of trust it gives rise to. In addition, the approach chosen by Castelfranchi (e.g. 2003) on studying normative issues in infosociety - permissions, obligations, power, roles, commitments, trust, etc. – and how computers might understand them, is an intriguing line of research. This work is approaches the trust issue from the more techical point of view, and aims to a formalisation of trust as logic (c.f, e.g. Falcone et al 2001 for more on this type of approach). In the most recent work of Castelfranchi (Castelfranchi et al 2006) and Camp (Camp 2006) we can also detect an interpretation of the current wide-spread interest on translating the real-world, often implicit, social networks into online explicitly expressed networks and modelling this.

5 Main Results of the Thesis and the Contributions of the Author

In this chapter, the main results of the work are summarized, and the contributions of the author are acknowledged.

5.1 Author's contributions in the thesis

The author has written the introduction, presenting an overview of the research done for the publications as well as a background for the studies. The introduction also entails a review of the related research in this area, bringing together a representative selection of trust research done in a wide area, including both actual HCI research but also those studies on the more technical side that come closest to the human side of trust.

[P1] Karvonen, K. (1999). "Creating Trust", Proceedings of the Fourth Nordic Workshop on Secure IT Systems (NordSec'99), November 1-2, 1999, Kista, Sweden, pp. 21-36

The purpose of the first user study was to find out about trust in the form of enquiring about users' current understanding of the security of the Internet as well as to learn about their behaviour patterns concerning their usage of the Web and areas that seemed relevant to this use. These include areas such as use of email, use of bank services, and use of credit cards. Qualitative semi-structured user interviews were chosen as research methodology. The users were also presented with a mock-up user interface for a web-based service (group 1) or with existing web services (group 2) to trigger conversation about ecommerce and security issues related to the transactions of money or private information online. The users were quizzed about their current knowledge of computers and banking habits, in order to find out about the possible similarities in behaviour in the case of using money regardless of the media. The notion of trust was discussed upon on many levels, including questions about trusting friends, work colleagues, a bank or a service-provider on the Web.

The first user interviews and evaluations took place in the first days of June 1999 and the second in the end of September 1999. In-between the results of the first user study were analysed and compared with existing literature. The second set of user interviews was then planned with the alterations mentioned above. The user study was planned jointly with Markku Laukka, who also conducted part of the interviews with the guidance of the author. The analysis and report of the results were the sole work of the author.

The outcomes of the user studies proved quite useful, and the study was repeated later in Sweden and Iceland. At the time of the study, such research was still almost non-existent, except for the work of (Jarvenpaa et al 2000), so it was one of the first of its kind. The Ecommerce Trust Study (Cheskin 1999), appearing at the same time, used partly similar nd partly different methodologies, and was producing results that corroborated the validity of the outcomes of the user studies. Choice of the methodologies was successful, and the analysis of the outcomes was accurate.

[P2] Karvonen, K. (1999). "Enhancing Trust Online", Proceedings of PhDIT'99: Ethics in Information Technology Design. Second International Workshop on Philosophy of Design and Information Technology, 16-17 December, 1999, Saint-Ferréol, Toulouse, France, pp 57-64

This work presents an ethical concern about trust promotion on a philosophical but also practical level. In the paper it is discussed, how ethical or unethical it is to try to enhance trust in the end users when in reality the online transactions can never be completely guaranteed. The work is completely based on the author's own ideas and work.

[P3] Nikander, P., Karvonen, K. (2001). "Users and Trust in Cyberspace", in B. Christianson, B. Crispo, J.A. Malcolm, M. Roe (Eds.): Security Protocols, 8th International

Workshops Cambridge, UK, April 3-5, 2000, Revised Papers LNCS 2133, Springer-Verlag Berlin Heidelberg 2001, pp. 24-35

In this work, the aim was to broaden the view from a protocol-centric approach towards considering the actual users, and to provide some initial requirements for future operating systems and user interface design in the area of authentication protocol design. To attempt this was new, and combining of human and machine trust was new and thought-provoking. The initial problem statement of the usability problems in this area is partly based on Nikander's previous work and ideas. All the actual usability problems were identified and analysed by the author. The paper represents the results of a tight co-operation of the respective authors and is a mutual outcome of their joint work, where both parties were contributing to an equal measure.

[P4] Karvonen, K., Cardholm, L., Karlsson, S. (2000). "Cultures of Trust: A Cross-Cultural Study on the Formation of Trust in an Electronic Environment", in
Proceedings of the Fifth Nordic Workshop on Secure IT Systems, NordSec 2000, 12-13 October, 2000, Reykjavik, Iceland, pp. 89-100

In order to see if the results would be valid in another country, and also to see how cultural variation might take place, the first user study was repeated in Sweden in 2000, with slightly different user group, different sites familiar to the Swedish users, in Swedish language, and by Swedish collaborators. The outcome of this study was that there was indeed quite a lot of difference which is likely to stem from cultural variation, but due to the different user group these results can only be considered as indicative. The user study was planned by the author on basis of the first user study, with some minor localisation type of changes made by the Swedish collaborators. The user study was run by Cardholm and Karlsson on the basis of detailed instructions provided by the author. The analysis of the findings as well as the transformation of the results into the format of a publication are the sole work of the author.

[P5] Karvonen, K, Holmström, U. (2000). "Expressing Trust", in Proceedings of NordiCHI 2000 (short papers), The First Nordic Conference on Computer-Human
Interaction, 23-25 October 2000, Royal Institute of Technology, Stockholm, Sweden. CD Proceedings, ed. Gulliksen et al. 2 pp.

This paper is based on Karvonen and Holmström's research work on the usability of trust mechanisms and identifies the challenges embedded in current trust mechanisms from a usability point-of-view. The current situation of the trust mechanisms was presented by Holmström. The usability aspects as well as the general framework of usability work in this area and their further analysis was done and written by the author, who is the main contributor of this paper. The aim of this paper was also to bring the trust and usability of security issues to the awareness of the Nordic CHI community.

[P6] Karvonen, K. (2000). "Experimenting with Metaphors for All: A User Interface for a Mobile Electronic Payment Device", in Proceedings of 6th ERCIM Workshop "User Interfaces for All" (UI 4 All), 25-26 October, 2000, Convitto della Calza, Florence, Italy, pp. 183-188

In this paper, a user interface designed in co-operation with and implemented by Markku Laukka for handling certificates was placed under two sets of usability tests, with different type of setting, in order to test the influence the question types would have on the test outcomes. The tests were designed, run, reported and analysed by the author alone. The author also participated in inventing the UI metaphors on which the design was based on. The UI design choices were based on the results of the user studies presented in publication [P1]. The paper presents these usability tests and represents the sole work of the author.

[P7] Karvonen, K (2000). "The Beauty of Simplicity", in Proceedings of the ACM Conference on Universal Usability (CUU 2000), November 16-17, 2000, Washington DC, USA, pp. 85-90

This paper presents a further analysis of the findings of the user studies of publications [P1], [P2] and [P3]. It presents novel and remarkable conclusions made on basis of the conducted studies on the importance of aesthetics for the trust formation process. At the time of this publication, the recognition of the aesthetics, and other emotional factors in HCI was only beginning, and this work is one of the first in reporting it among (Tractinsky 1997, 2000). The work was done solely by the author.

[P8] Karvonen, K. (2001): "Designing Trust for a Universal Audience: A Multicultural Study on the Formation of Trust in the Internet in the Nordic Countries" (invited paper), in the Proceedings of the First International Conference on Universal Access in HCI (UAHCI'2001), August 5-10, 2001, New Orleans, LA, USA, Vol. 3, pp. 1078-1082

To further test the effects of culture on trust-formation, the original user study, with some slight moderations and with a smaller user group, was again run in Iceland in 2000. Now, the cultural variation seemed even stronger and the trust-formation process appeared to be quite dissimilar from that of the Finns and Swedes: the cultural factor in trust-formation was quite evident, and the cultural variation seemed to be great.

Further, on basis of the analysis of the users studies conducted in the three countries, the upsurge of recommendation-based systems for formalising trust expressions and for making trust decisions, seems a natural path for the trust-formation: one of the major outcomes of the work at hand is that also in technical environments, humans trust, first and foremost, other humans, not machines. Providing users with ways for embedding existing social networks to the online environment is a natural application of this outcome (see also Camp 2006, Bonhard et al 2006).

The user study in Iceland was planned, run, reported and analysed solely by the author.

[P9] Karvonen, K., Parkkinen, J. (2001). "Signs of Trust", Proceedings of the 9th International Conference on HCI (HCII2001), August 5-10, 2001, New Orleans, LA, USA, Vol. 1, pp. 1076-1080

In order to better understand the meaning and effect of the visual elements of web design on trust formation, the author invited a colleague who had expertise in semiotic analysis to jointly analyse the identified research problems from a semiotic point-of-view. This analysis proved to be quite fruitful, leading to a better understanding of the symbolism of the online elements. The work was done in tight co-operation jointly by the both authors. Parkkinen provided the semiotic framework and the author provided the data to be analysed and fully participated in the actual analysis and wrote the publication.

5.2 Main results

The main results of the work at hand can be divided into the following areas:

1. Understanding of the affecting factors of trust-formation process in online situations;
2. Identifying the key issues in trust and usability of security;
3. The effects of design on trust;
4. How to apply methods of usability and user-centred design to the study of trust.

These are elaborated on next.

5.2.1 Understanding of the affecting factors of trust-formation process in online situations

The answers from our interviews indicate that the affecting factors are in making trust decisions in online ecommerce use situations, in order of assumed importance:

0. personal attitude to others (trusting/distrusting) and cultural factors
1a. previous experience from the specific web-shop, or 1b. real-life vendor
2a. known brand, or 2b. trustworthy design
3a. right price, or 3b. secure payment method,
4. right delivery conditions,
5. financial or reputational risk on service provider
6. privacy policy.

A possible chain of decisions made by a customer before a purchase is presented in **Figure 2**. To start with, previous experience from a specific web-shop seems to be a conclusive factor. The experience does not necessarily need to be personal; it could come from trusted friends or media. Even so, it seems like personal experience has the strongest influence on the consumer, especially over time. If a person has successfully completed a purchase in the past, the customer would not hesitate to do business with the same service provider again. This time the *price* of the product would be a more decisive consideration.

When considering doing business with a web-shop for the first time, reputation and previous experience of the company is very important. A well-known brand is crucial for attracting a potential customer. Design of the web site seems to be most important when the service provider is unfamiliar. A web site of an unknown service provider must give a professional impression and immediate communicate their services. Otherwise, the user will move on. In these circumstances is it also more important to provide quick download of pages and easy navigation, than it is for known providers. When the consumer is familiar with the company behind the web site, the kind of products they have for sale is not an issue. The customer knows beforehand what to look for and is probably visiting the site with a special purpose. When doing business with an online shop the customers expect prices to be low. As it is easy to compare prices on the Internet, a shop with higher prices than others will most likely have problems attracting customers. Another factor of interest for our respondents was delivery conditions. There is a demand for speedy delivery, preferably all the way to the customer's front door.

At the bottom of the considerations, comes the question of secure payment for deciding whether to use a service or not. This is not due to lack of importance but more to the fact that the customers do not consider doing business at all with a service provider that does not let them pay by invoice. This reality is known to Swedish service providers. In our web site evaluation, there was only one foreign service provider (Amazon.com) included and the question of paying over the Web was never really an issue. The respondents themselves concluded that what they actually do when they are doing business online is what is traditionally known as mail ordering.

In the ECommerce Trust Study in 1999, one of the fundamental elements when communicating trust was seals of approval. One condition for these seals to be of any relevance at all is that they be well known and noticed by the customer. This was not the case among the respondents in this study. Hence, the conclusion must be that seals of approval have little impact on communicating trustworthiness among Swedish and Finnish web consumers, at least for the time being.

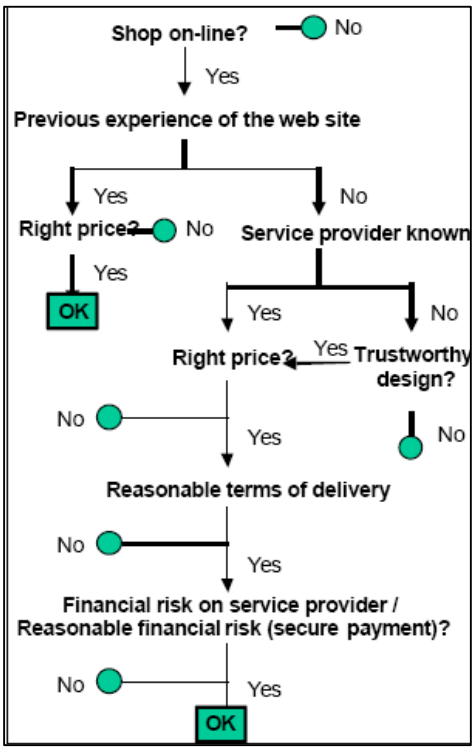


Figure 2: A flow chart of the transaction process and the trust decisions

Users were willing to trust *established real-life vendors* also online, especially if they were controlled by special legislation, e.g. banks. Users would ask for help from the *people they knew* for making the trust decision. Further, the information provided by mass media and the services themselves was considered *incomprehensible* or irrelevant in most cases. The sources of trust were manifold, but both *other people's experiences* and *trust in existing institutions and real-life vendors* came clearly out as the most important criteria for trust. These were the most important sources for initial trust. As experiences with a given service accumulated over time, the trust was also based on *previous successful encounters* with the service at hand.

Trust was not an explicit concept for the users. They would in most cases show trust or lack of trust via willingness to interact or withdraw from interaction with a given service or any online transactions. Users would, in the interviews, most frequently mention ecommerce and email usage as the cases where trust would be an issue, when probed for it. Since trust was not an explicit concept for the users, they had a hard time explaining about the meaning of trusting or distrusting. Users would express the trust/distrust as a feeling that something is or is not "right". Trusting was shown by willingness to interact with the given service.

5.2.2 Identifying the key issues in trust and usability of security

Considering all the research done by us and by others, we can identify the following four kinds of problems in making computer security usable as most crucial:

1) People are not interested in computer security *per se* – they are only interested in what it enables.

2) People do not understand security technology, concepts or terms – even if they were interested.
3) People do not behave rationally and do what is best for them – even if they did understand it.
4) People do not trust machines, but *other people*.

The interpretation of these challenges can be rather straightforward. People are not interested in security as such, so automation to a certain extent will be a good idea. Another approach will be to try to think of ways to make it more interesting in some way. The fact that people do not currently understand what computer security is all about, is easier to tackle, in a way: we need to find better terminology to use and work hard on providing easy-to-understand information about security to the online users. Further, we must take care that the information provided covers the areas they are interested in.

To further emphasise the *human* in the "human problem" we can, on basis of the conducted research, rewrite the list provided by (Shneier 2000) as consisting of the following six corner stones:

1) how people perceive risks and what they perceive as risks
2) how computer security could be easier to memorize and to learn
3) how people could trust computers and the networks and how they could express this trust in an easy and understandable way
4) what part of the computer security could be automated and what cannot be automated; the latter must be communicated to the user in an intelligible, easy-to-understand way
5) how people could learn about computer security and even be interested in it
6) how people could assure their privacy level to be the one they want and need.

The various research threads of trust research, stemming out of various sources is descriptive of the intricacy and complexity of work on this area. It is not likely that we will be witnessing answers to these problems too soon. Further, new problems arise as we go along sorting out the old ones.

The irrational behaviour of humans is one of the key points to be kept in mind when designing usable security: if we design for some sort of imaginary "model citizens", who always behave well, think carefully about the consequences of their actions, and act in their own best interest, we end up creating unrealistic application, intended for these virtual beings. Instead, the systems designed should be based in the real world needs and capabilities of the "average man". The fact that trusting decisions are often implicit, provides big challenges for guiding the users to the "right path", for they may be unwilling to listen, and unaware of why they feel so strongly for something

The fact that people tend not to trust machines, but place their trust in other people, is also a crucial conclusion. The usage of online services may not even be really tied to a trust decision in a way: if user wants something badly enough, they will engage even in transactions they perceive as risky. However, there may not be any trust behind this decision. The upsurge of recommender systems, based on reputation have been so successful just because of the fact that it enables users to trust other users – an outcome easily deductible from an analysis of the results of the user studies presented here.

5.2.3 The effects of design on trust

During this research, a surprising outcome was discovered. The aesthetics of the services used seemed quite significant for the trust decisions [P7] and [P9]. This was an unexpected result, but was at the same time implicit in previous work (e.g. Cheskin 1999), verified by other

research groups around the world, especially by (Tractinsky et al 2000), later by (Norman 2003) and verified experimentally by e.g. (Riegelsberger 2003) and (Lindgaard et al 2006) and further developed by e.g. (Wang 2005), (Yang et al 2005). During the recent years, understanding the importance of aesthetics has become mainstream HCI, and is currently investigated by many. The outcomes of these studies, along with the understanding on the trust mechanisms behind the surface, can be used for building up instructions on how to create *trusted design*.

Based on our work, we can now give some design rules for trustworthy design, even if this was not one of the goals of the study at hand and has been dealt with more extensively by others, especially (Egger 2003) and (Tractinsky 1999, 2000, Cyr 2006, Kim et al 2003).

The outcomes of this work have further corroborated the outcomes of especially (Egger 2003), as regard how to design for trust. On basis of our work, we can state that a smart security designer should take into account all the factors discussed above and make security as carefree as possible at the same time, but also visible to some extent and persuasive as well. Special attention needs to be paid to the logic and ease of navigation in during the payment process. The basic requirements for trusted design, thus, include the design to be at least the following:

- *Carefree*: Users do not care about security as primary goal. The feel of the design in security prone applications should be that of easiness, even fun, and speak the user's language.

- *Appropriate*: Design must support content. No matter how fine the finished design that we may create, it may still end up connoting untrustworthiness – this will happen if the chosen design style is not in concordance with the content of the service. What this means is that the design of, say, a Web bank should be different from the design of an entertainment service site. When users were describing their trusting attitudes, they would refer to this as saying, for example that “a bank has to look like a bank”. This means that a design for a bank needed to denote things such as seriousness, professionalism, and solidity. However, how these design ingredients should be interpreted is hard to pinpoint (Ecommerce Trust Study 1999, Surendra et al 1999, Lindgaard 2006).

- *Familiar*: Common look for e-vendors operating in same business areas will benefit all. In practice this means, for example that in order to succeed, resemblance across Web-sites providing similar services is likely to enhance the trustworthy appearance of all those vendors. Existing research by others has also shown that this kind of similarity will promote the feeling of familiarity in the consumers (e.g. Lindgaard 2006). The operational area of the e-vendor will create implicit expectations in the consumer as regards the Web design. If these expectations are met, the site is evaluated as more trustworthy than otherwise would be the case. Co-operation among vendors active in the same area might prove beneficial for all parties. Users must immediately see that the site is an ecommerce site, plus where and how to buy. If all the banks, all the book stores, and all the travel agencies etc. operating online had a similar appearance (inside each group), the consumer would find it more easy to understand which areas they operate on, what to expect from these services, and how they operate.

- *Usable*: The site must also live up to the common ISO usability standards of effectiveness, efficiency, and satisfaction – as any other service should do. In web usability, for example, the kind of basic usability principles and practices such as described in (Nielsen 1993) should also be followed, when possible. Ease of interactions, based on good usability, forms the basis for all good user experiences online.

- *Creating flow:* The transaction process should be swift from start to finish. If there are break-ups and considerable waiting periods in getting from one part of the service to the other, in the loading of pages, users will become suspicious of the overall competence of the service. Especially in the actual transaction procedure, delays are quite intolerable for most users, who will shy away from slow or cumbersome transactions, wondering, "What is going on in the background" [P1]. If the generic, acceptable waiting time from usability point-of-view is about 10 seconds (e.g. Nielsen 1993), in the transaction process the tolerance is far smaller, probably practically measured in sub-seconds.

The suggestion for co-operation and similarity online across businesses in the same area is a bit uncommon thinking in the world of Web design. Creating a 'fancy' and distinguishable design has been one of the most sought-after qualities of desirable design. Even though such pleasantness should by no means be abandoned, the similarity aspect should also be encouraged/developed/nurtured. Differentiation is appropriate for fun and for artistic purposes – however, for serious business purposes it is not. Such similarity also promote learnability of the site's structure and functionality, since transfer of previous experience will become possible. Perceived similarity is a proven trust promoting factor elsewhere (Fogg 2003), so probably also here.

This conclusion goes against the current trend to praise individuality and to try to differentiate from competitors with all means possible. In the Web environment, this approach has meant that every Web page tries to be different from others. Since the logical elements of the sites of businesses in the same area are, however, more or less the same, similarity cannot in fact be easily avoided even when not actively being pursued – which might, after all, be a good thing.

The solution so far has been to introduce differences in the level of colours, flashy animations, and introductory tours before entering the main site. This policy has proved to be harmful for the success of ecommerce. In a way, adopting this differentiating policy has meant, from the consumer point of view, hiding the true and apparent functionality and purpose of the site from the consumer. This has led to confusion about the purpose of the sites and their possibilities. This, in turn, has led to loss of consumer trust towards the online vendors. By abiding to the design rules presented above, it will, however, be possible to overcome these weaknesses in contemporary Web design approaches, and to create trustworthy design for e-vendors. Perhaps we should not call it Web design in the first place, but rather, ***ecommerce design*** – with rules of its own, in part different from Web design rules (see also Egger 2001, Kim et al 2003).

We have found out that at least the Nordic users preferred "simple design". In the future, it would be interesting to investigate further into *what kind of simplicity* would be right for creating trustworthy design. In the study by (Lindgaard et al 2006) it became obvious that what is simple is not that simple (sic). Graphic designers often complain that usability experts always want design that is too simple, which they commonly interpret as boring. Simplicity in this sense is a kind of "stripped" simplicity – the design is stripped naked of all fancy features, colours, and flashy, moving objects. Is this what users really want? Alternatively, could there be a second kind of simplicity that they actually mean, "designed" simplicity – clear, and "clean" like the Swedish users wanted, but in a stylistic and beautiful way that does not lessen the pleasure provided, even if it lessens the elements the page consists of? We think it is this latter form of simplicity that is asked for. However, simplicity cannot be advertised to end-users under this label – it is a well-known human phenomenon that simplicity is not desirable since it is not socially acceptable and because it does not reflect a self-image one could be proud of (e.g. Norman 1986). People want more: more buttons, more functionality, and they want to see themselves as "experts", above the average. They do not want to be labelled as those who use "simple designs" (Norman 1986). In any case, the importance of aesthetics in making trust decisions has become evident, and needs to be studied further, as is already happening.

5.2.4 How to apply methods of usability and user-centred design to trust

In the user studies in this work, there has been a pursuit to try out various methods, and see which would seem to prove best results. However, questionnaires were left out of the study on purpose, as were expert interviews: the first due to the fact that such research were already ongoing and could be used for comparison of the outcomes; the second due to the fact that in the scope of this research, the interest was directed only on the 'average men and women' – users *without* expertise. Also, we wanted to try to simulate real use situations as far as possible: the usage of demo services and actual services were observed and analysed. This work was combined with interviews and usability testing of the created UI designs (see **Figure 3**).

These methods seemed to prove best results when doing research under the described circumstances. On basis of quality of the outcomes, we would recommend as most suitable methods for studying online trust a mixture of methods, with an emphasis on qualitative methods stemming mainly from ethnography (observing usage, interviewing, participatory design), enhanced with the traditional usability engineering such as usability evaluations, supplemented with some type of experimental test setting (e.g. Lindgaard et al 2006, Riegelsberger 2003, Brostoff and Sasse 2003) questionnaires (e.g. Fogg 2003, Cheskin 1999), or expert interviews (Cheskin 1999, Tang et al 2003) to validate the findings. The Grounded theory framework as applied by Sasse et al might prove useful also in this context.

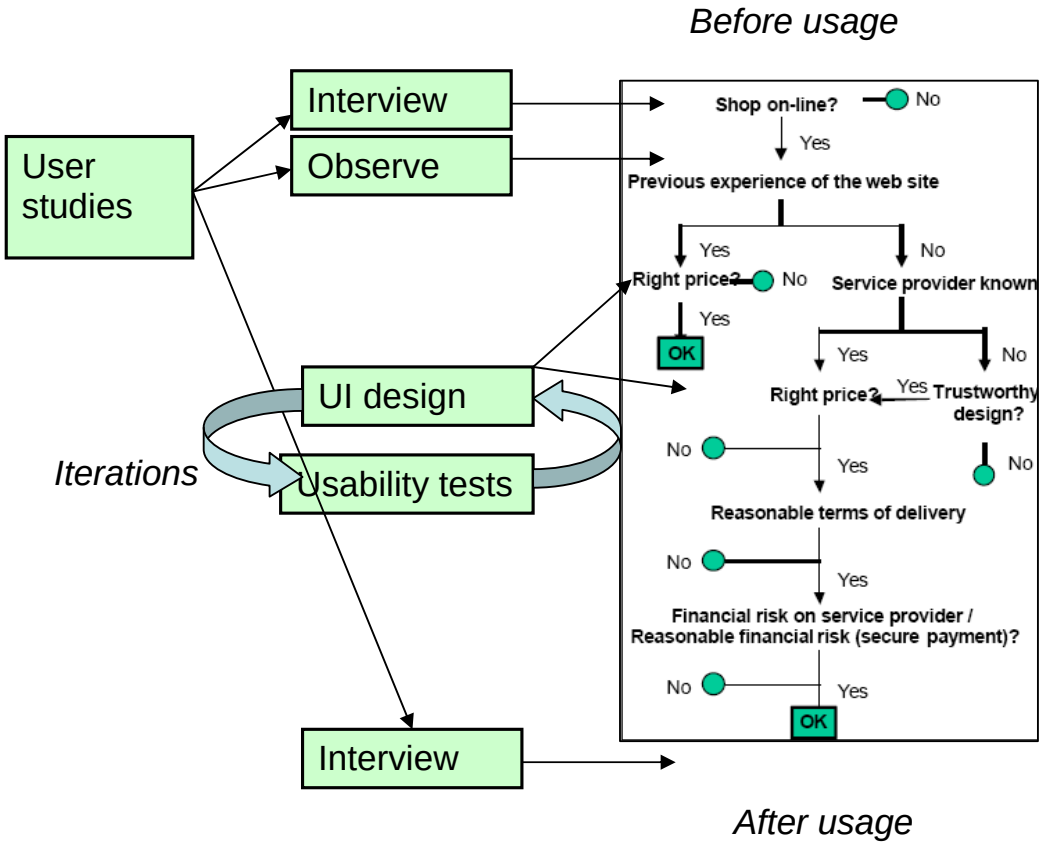


Figure 3: Applying usability methods for studying trust decisions

6 Conclusions

During the research, it has become obvious that still today, the average user does not know much about the security risks nor the security techniques that exist. Thus it is practically of no use to give her information about it, at least not if the information given is too complex, and there is too much of it. For all these reasons, as much of the security as possible should be automatically taken care of on behalf of the user, while at the same time retaining its visibility to some level and enabling the feeling of being in control, if not totally responsible, of each use situation. The user truly is the weakest link in securing a system. Most security mechanisms are far too difficult for the average user to manage. Thus all trouble for making a system safe is in vain if the user is left in charge of the security. Yet there is a need to show to the user in some way that her security has been taken care of. Some kind of feedback is clearly needed. The design of the user interface for any system should, then, take all these things into consideration.

There are really no recognised exemplars of good user interface design for secure user interfaces as yet (Whitten and Tygar 1998, Salam et al 2003; Camp 2006 will be interesting to judge). The six primary components to promote trustworthiness in the user listed by the Ecommerce study (Ecommerce Trust Study 1999) were one of the first to even try this. The studies reported here verify, to the most part, the findings of that study. The brand name of the service provider was one of the key features to enhance trust in the users also in our studies. It applies to most other components, except for the seals of approval. These were quite unknown to the users who participated in our user studies, and once they were explained what they were about, users were very doubtful about their true value. After all, they can be seen as ‘mere images’, too (e.g. Camp 2006).

In order for all this research to be useful, quite a lot still needs to be done. First, it is not at all clear how the various kinds of trust relationships and their expressions could be turned into certificates or other kinds of signed documents, if we think about solution with a centralised architecture. Second, the actual user expectations and their probable reactions to various kinds of automated trust evaluation mechanisms should be evaluated. Third, even the concepts of trust and trustworthiness need more clarification, both in the formal sense and especially in a language understandable to the average user. Even if the reputation-based systems working via recommendations seem to be dominant at the moment, they too are not without problems in the area of trust. The current solutions, such as eBay, rely, for the most, on the fact that people are happy to turn a blind eye towards the actual risks of the system and what lacks in the security.

It still holds that one of the major challenges in creating more usable computer security is the fact that most users do not find it interesting. It is a necessity, often traded off if need be, not an end in itself (e.g. Sasse 2003, Yee 2005, DeWitt et al 2006, Schechter et al 2007). Getting users to care enough about their own security is one thing, getting them to want to learn more about is something else altogether. When it comes to computer security, users tend to get scared and shy away from an area they find too complicated to grasp. This is true even for those users, who are otherwise into new technology. All the users wish to know about computer security, is that *exists* – that they are *safe*.

6.1 Future Work

In this subchapter, we present some suggestions for possibilities for continuing the work on studying trust.

6.1.1 Extending the probe on cultural variation

The clear differences in user attitudes affected by cultural factors are one of the cornerstones of the current study. Repeating the study with Finnish users, Swedish, and Icelandic users will prove interesting results in how time and the new emerging systems have changed the attitudes in these three countries. Extending the study to more countries would also be interesting. The work on repeating the study in Nordic countries has in fact already started with Finnish users (Karvonen 2007), and plans to extend it to include other countries outside the Nordic region is also underway. The initial studies suggest that even when users, on one hand, seem to have become bolder in their online interactions, on the other hand, the new threats of identity theft, for example, are again forming new obstacles for online interactions (e.g. Camp 2004). In the end, even when users are interacting more actively in online transaction situations, the means to protect oneself, the feelings of distrust, and need for more information have more or less remained the same. Since there are also novel factors affecting the situation such as the flourishing of recommendation-based systems, the outcomes of the whole study are hard to foresee in advance.

There are many ways to pursue further in studying trust. One possibility to continue this line of study would be conducting more or less the same interviews with individual users from various other cultures, as well as observing these users in real use situations similar to the ones described here – performing tasks on the existing, security-prone services, and evaluating their trustworthiness in today's climate of trust. In doing this, we would expect to find some differences to previous findings, due to changing behaviour patterns in the accumulated timeframe. Special attention could be paid to the theme of "simple design" - what this might mean in different cultures and different users, and what the design wishes of various groups and subgroups might be. Good example of this are the findings of the study at the AT&T Labs-Research (Cranor et al 1999, see section on **Privacy**) on Net users' attitudes towards privacy, where it was concluded that users could be divided into at least three groups according to their privacy assessments. All these different groups seem to require different user interface designs, emphasizing different aspects of the underlying systems' security. If this still holds today, remains an open issue.

The question of cultural variation continues to be an interesting and pressing theme. On a truly global environment like the Internet, to fully succeed in creating services that are understandable to all their international users is not possible without taking into account the cultural variation in the attitudes, values, likings, aesthetical taste and trust structures of users across continents (Jarvenpaa et al 1999, 2000, and Tractinsky 2000 for a number of references). On the other hand, a *global convergence* might also happen. The global culture of the Internet might start to overcome the local cultures and expectations they bring along, as the usage is mature enough. For making *global research* across cultures in a new way, (Masten and Plowman 2003) are using *digital ethnography*, where the basic assumptions include such globally more or less similar techno-culture as generic framework[6]. It remains to be seen how successful this approach will be.

6.1.2 The role of design and aesthetics for trust

Still unclear remains also the component of "presentation". It only states that quality design connotes professionalism. However, what, then, is quality design? In our studies, the users mentioned *clarity* as one of the key features that made visiting a web site most pleasurable. By clarity, it was meant that there were just a few elements on the screen, few commercials if any and navigation was found to be straightforward and easy. It is possible, however, that

[6] The main emphasis in this article is, however, on trying out a new research methodology for conducting user studies on geographically distributed users simultaneously.

these findings reflect the Finnish user specifically and thus the results cannot be generalised to a more international group of users. Previous research from field such as aesthetics that have over time created an understanding of issues related to "quality", "pleasurable" and, naturally, "aesthetic" would likely be useful to study such issues, and this possibility was introduced in a separate study [P7]. Indeed, later on the study of the meaning and significance of aesthetics has become an important trail in current study of trust and within the field of UX (e.g. Lindgaard et al 2006, with a good reference list and recent findings on studying the aesthetic ingredient; see also Kim et al 2003).

These differences in design do not touch just the language but also the way people with different cultural backgrounds perceive privacy, security and what or who they can trust and on what basis, and the aesthetic question must be dealt in concordance with the study on cultural variations in trust-formation. The culture specific traits of both the design and the service must be recognised and translated along the language (e.g. Hawkings 1999). It is not enough to change the language of the user interface; the changes must go deeper than that.
A Trustmark displayed on the home page of the service provider may inform the visitors of the security practices conducted at that site, but what is considered assuring enough may vary greatly across different cultures. This point was also investigated further, to some extent, by repeating the user studies reported here in Sweden [P4] and in Iceland [P8]. Indeed, differences between the neighbouring countries, Finland and Sweden appeared to be rather small, whereas Icelanders exhibited rather different trusting behaviour than the other Scandinavians [P8] – so there was a considerable amount of heterogeneity already within geographically rather small area.

6.1.3 Making security more interesting, or even fun

We have seen how in security, we are faced with users who are not only reluctant but also scared, bored and bothered by our goal of providing them with more security. It is a good question, how to turn the wheel. However, examples of funny and entertaining computer security information also exist. When computer security information is targeted at children, things can change drastically. A good example is Disney's web pages (http://disney.go.com/surfswell/index.html), where children – and why not their parents – can delve into "Adventures in Internet Safety" in "Surf Swell Island". There, the user is wandering through "virus cave", "privacy falls", and "temple of tact", learning on the way the basics of computer security and online etiquette via answering some simple questions and receiving immediate feedback for right and wrong answers.

The approach that turns computer security into a quiz and a game could provide some ideas for how to present the computer security issues also to grown-ups. Even when using cartoons and animations may not be the best way to convince users and promote trust in the advice given (Cheskin 1999), when well applied some of the idea might lead away from the technical jargon and towards an easy-to-use set of security information and advice. In addition, cutting the information into smaller chunks on every level is advisable (Ackerman et al 2005, Yee 2005, Uzun et al 2007).

6.1.4 The Emotional consumer

Consumer studies come close to trust studies within HCI when the object of study is trust and behaviour in the context of online shopping. Users, in the role of consumers, are likely to act differently than in situations where money is not an issue, and the theories of marketing research and consumer research have a lot to give. I hope that we will witness an upswing in studies combining these approaches.

Introducing personal psychology and consumer satisfaction are closely related to the recent major trend inside HCI: the study of feelings as an integral part of this interaction. This trend has several sources. Firstly, the previous concentration on the cognitive, rational factors in how humans behave was simply too narrow in scope. That paradigm was naturally born out of the earlier concentration on work environments, where computers first were used. Taking the affective side of human into account was a natural step, as the field as a whole has matured (c.f. Picard 1997 for groundbreaking work towards this expansion of the field in scope).

Secondly, the study of HCI has left the office and entered the user's spare time, treating users of machines not only as workers but also as individuals with personalities, likings and dislikings, and so on. Studying the affective side of HCI follows naturally with these new directions. When the computers are used not only to accomplish chores dictated by others, but as tools for personal fulfilment, for socializing, for art-making – it is no longer enough to study just the cognitive side of the human participant of this interaction in order to improve effectiveness. Further, considering this side sets novel requirements of novel types for the machines possibly unheard of before, and sets the development of these devices towards new directions. The applications run on these systems these days may be immersive games or chats or dating services that by nature are designed to entertain and deal with feelings, more so than to appeal to the information processor inside the brain. Even more, this information processing is no longer treated as a property of the brain alone, but intelligence needed in rational decision-making is constantly detected also elsewhere (e.g. Lindgaard et al 2006).

This new approach is, however, built on the existing knowledge on 'traditional usability' of effectiveness, efficiency and satisfaction – this basic level of usability, consisting of things like memorability, learnability, and so on, is needed as basis for the emotional level to be built on in order for it to be possible and to work. Emotion-provoking, immersive experiences need the traditional aspects of usability as their groundwork in order to be able to fulfil their goals, i.e., to evoke feelings. The development from physical ergonomics some 60 years ago to today's analysis of the entertaining elements of computer games and online environments and virtual communities seems long yet natural and follows a logical path.

In the light of the above, it is also natural, then that also the in the study of trust the emotional, irrational side has gained a lot of attention. As we have seen, trust is by its very nature built in part on cognition and on the other part on emotion. The trust research has not yet, however, been integrated too well with the emotion research inside HCI, but has remained more or less as an isolated field.

6.2 Epilogue

Even if there are many problems in trust that remain unresolved, online shopping seems to have undergone a major shift from distrust to trusting (or carefree) behaviour. This becomes inevitable by current consumer studies on users' online buying behaviours. For example, the Christmas study ordered by Deloitte in 2005[7], showing an outstanding growth in the amount of gift shopping among British consumers (see **Table 2)**.

In other words, in the U.K over 50% of the consumers was at least planning to purchase gifts and services online for Christmas 2005. The reasons behind choosing to conduct shopping online, are manifold, ranging from better prizes to better availability, and so on. **Table 3** summarises these factors.

[7] http://www.deloitte.com/dtt/press_release/0,1014,sid%253D2834%2526cid%253D103623,00.html

Year	Consumer use of internet for purchasing gifts
2005	51%
2004	32%
2003	29%
2002	22%
2001	12%
2000	11%
1999	8%
1998	2%

Table 2. Seven years of the Internet for Christmas gift shopping (Deloitte 2005)

Year	**2001**	**2002**	**2003**	**2004**	**2005**
Better quality goods/ services	4%	4%	3%	3%	2%
Easy to return goods	0%	5%	0%	3%	2%
Easy to get credit	0%	3%	2%	0%	0%
Good customer service	2%	7%	0%	1%	2%
Convenient	35%	19%	-	-	-
Quick delivery to home	14%	15%	11%	11%	10%
Browse for products/ services without hassle	15%	17%	16%	16%	12%
Saves time	20%	16%	27%	22%	30%
Saves money	-	11%	19%	23%	20%
Prefer the online shopping experience	-	-	2%	3%	3%
Other	11%	3%	12%	10%	14%
Don't know	0%	0%	8%	9%	5%

Table 3. Reasons for using the Internet (Deloitte 2005)

According to the Deloitte study, Internet is alluring especially to such users who have learned that a low price does not equal low quality. One of the major ingredients in online shopping creating competitive edge is still low price, and saving time. Using Fogg's terminology, the trust is here based on "Earned Credibility": the users have first-hand experience, extending over time, about doing online transactions..

This positive trend of growth in online shopping is threatened, especially in the U.S., by the fear of *identity theft*. This phenomenon and its relation to local and global legislature should be investigated soon within trust research, since this fear might jeopardize this growth. Some examples of work in this area are already emerging (e.g. Camp 2004). Why the convenience factor has disappeared from the factors having an effect, was not explained in the study outcomes, unfortunately. However, it is interesting to learn that the shops flourishing online and making the best profits are multi-channel vendors, instead of pure online merchants. According to the study, women were more likely to use supermarket (54%) and high street store websites (62%) than men were, where as men would use manufacturers' sites more often (48%). This is potentially bad news for "pure play" online retailers. In the wake of the recent focus on so-called "dual pricing" for online trading, it could be seen as a further boost for established multi-channel retailers.

The user interface design for secure user interfaces is still in making, as is proper understanding of what is trust. To get to the core of trustworthy design has proven a hard nut to crack. Thus, as the users' expectations vary quite a lot, the mechanisms are not quite there yet, and it is unclear how the implementation of such mechanisms would affect the design and structure of operating systems and user interfaces, this work has not progressed too far as yet.

However, we wish that the work presented here would help in leading to new ideas and points of view about how to build easy-to-use security for the online world and how to deal with its users, preferably eventually leading to an Internet that is more secure, in practice, than the current one. Understanding the making of unbroken security on a general, deeper, device-independent level, namely, understanding what makes people trust other people or machines and how this trust builds, may serve as key in understanding what kind of security threats and other trust issues we will confront also in the future. Taking a closer look at the counterpart of trust, the *distrust* might be fruitful.

It has become clear that usable security is hard, and in the future, the *people* still present the biggest challenge to the designer of the computer security systems: users do not always know what is in their best interests. This is also the case in the real world, where many decide to place their trust in fortune-tellers and horoscopes even in important life-forming decisions. However, the studies reported here have clearly improved our understanding of the differences between the trust as expressed by humans and between humans, as compared with the traditional technical expressions of trust. I hope that the results of these studies will help to bring these two closer to one another in the future, and have managed to show the true value of the outcomes received by executing the user-centred approach in usability of security. The ultimate aim of this work is to show way and provide means to more usable security – to provide building blocks for the bridge between human and machine trust, transforming the "human problem" in security into the "*human challenge"*.

7 Bibliography

1. Ackerman, M.S., Mainwaring, S.D (2005): Privacy Issues and Human-Computer Interaction. In: Cranor, L. and Garfinkel, S. (Eds), Security and Usability. Designing Secure Systems that People Can Use, O'Reilly 381-400

2. Adams, A and Sasse; M.A (1999a), "Privacy Issues in Ubiquitous Multimedia Environments: Wake Sleeping Dogs, or Let Them Lie?", Proceedings of Interact '99, IFIP TC.13 International Conference on Human-Computer Interaction, 30th August - 3rd September, 1999, Edinburgh, UK, pp. 214-221

3. Adams, A & Sasse, M.A (2001): Privacy in Multimedia Communications: Protecting Users, Not Just Data . In A. Blandford, J. Vanderdonkt & P. Gray [Eds.]: People and Computers XV - Interaction without frontiers. Joint Proceedings of HCI2001 and ICM2001, Lille, Sept. 2001. pp. 49-64. Springer

4. Adams, A and Sasse, M.A (1999b), Users Are Not the Enemy, *Communications of the ACM*, Vol. 42, No. 12, December 1999, pp. 41-46

5. Anderson, R (2003): Cryptography and Competition Policy - Issues with 'Trusted Computing', in Proceedings of PODC'03, July 13-16, 2003, Boston, Massachusetts, USA. ACM Press, pp. 3-10

6. Anderson, R.J (2001), Security Engineering. A Guide to Building Dependable Distributed Systems, Wiley & Sons, U.S.

7. Araujo, I.& Araujo, I (2003): Developing Trust in Internet Commerce, in Proceedings of the 2003 conference of the Center for Advanced Studies conference on Collaborative Research, October 2003.

8. Basu, A and Muylle, S (2003): Authentication in E-Commerce, in Communications of the ACM, December 2003/Vol. 46, No. 12 ve, pp. 159-166.

9. Bellman, S, Lohse, G.L. and Johnson, E.J (1999), Predictors of On-line Buying Behaviour, *Communications of the ACM,* Vol. 42, No. 12, December 1999, pp.32-38

10. Benassi, P (1999), TRUSTe: An On-line Privacy Seal Program, *Communications of the ACM,* Vol. 42, No. 2, February 1999, pp. 56-59

11. Bertino, E, Khan, L, Sandhu, R and Thuraisingham, B (2006), Secure Knowledge Management: Confidentiality, Trust, and Privacy, IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans, 36(3):429-438, May 2006

12. Bertino, E and Sandhu, R (2005): Database Security - Concepts, Approaches, and Challenges. IEEE Trans. Dependable Sec. Comput. 2(1): 2-19, 2005.

13. Beth, T, Borcherding, M, and Klein, B (1994), Valuation of trust in open networks, in *Proceedings of Computer Security--ESORICS'94,* Brighton, UK, 2-9 November 1994.

14. Blaze, M, Feigenbaum, J and Lacy, J (1996), Decentralized trust management, in *Proceedings of 1996 IEEE Computer Society Symposium on Research in Security and Privacy*, Oakland, CA, May 1996.

15. Blaze, M. et.al (1999): The KeyNote Trust-Management System Version 2, RFC 2704, September 1999

16. Blaze, M, Feigenbaum, J, Ioannidis, J, and Keromytis, A (1999). The role of trust management in distributed systems security, in Secure Internet Programming, vol. (1603) of Lecture Notes in Computer Science, pp. 185-210. Springer-Verlag Inc., New York, NY, USA.

17. Blythe, M.A., Monk A.F., Overbeeke, K., Wrigth P.(2003). Funology - From Usability to enjoyment. Human-computer interaction series 3, Klüwer Academic publishers

18. Bonhard P. (2005). Who do I trust? Combining Recommender Systems and Social Networking for Better Advice, Position paper for workshop: Beyond Personalization 2005, IUI05, Jan. 9, 2005, San Diego, California

19. Bonhard P., Harries C., McCarthy J., Sasse M. A. (2006). Accounting for Taste: Using Profile Similarity to Improve Recommender Systems, in Proceedings of CHI 2006, Montreal, Canada, 22-27 April 2006

20. Bonhard P., Sasse M. A. (2005). I thought it was terrible and everyone else loved it - A New Perspective for Effective Recommender System Design, in Proceedings of the 19th British HCI Group Annual Conference, Napier University, Edinburgh, UK 5-9 September 2005, pp. 251-261

21. Bonhard P, Sasse M. A. (2006). Knowing me, Knowing you - Using Profiles and Social Networking to Improve Recommender Systems**.** In BT Technology Journal, Vol. 25, No. 3, July

22. Brostoff, S & Sasse, M.A (2000). Are Passfaces more usable than passwords? A field trial investigation. In S. McDonald, Y. Waern & G. Cockton (Eds): People and Computers XIV - Usability or Else! Proceedings of HCI 2000 (September 5th - 8th, Sunderland, UK), pp. 405-424. Springer.

23. Brostoff, S & Sasse, M.A. (2003). Ten strikes and you're out": Increasing the number of login attempts can improve password usability. Paper presented at the CHI 2003 Workshop on Human-Computer Interaction and Security Systems, Ft. Lauderdale, April 5-5, 2003

24. Bunnell, J, Podd, J, Henderson, R, Napier, R, Kennedy-Moffatt, J (1997), Cognitive, Associative and Conventional Passwords: Recall and Guessing Rates, *in Computers and Security, vol. 16 no. 7 (1997),* pp. 645-657

25. BusinessWeek/Harris Poll (1998), Online Insecurity. http://www.businessweek.com/1998/11/b356107.htm

26. BusinessWeek/Harris Poll (2000), The Growing Threat. http://businessweek.com/2000/00_12/b3673010.htm

27. Bødker, M., Christensen, M.S., Jørgensen, A.H.J.(2003), Understanding affective design in a late-modernity perspective, In proceedings of DPPI Pittsburgh, ACM press, pp.134-135

28. Camp, L.J, (2000). Trust & Risk in Internet Commerce. MIT Press, Winter (Cambridge, MA)

29. Camp, L.J. (2006). Reliable Usable Signaling to Defeat Masquerade Attacks WEIS 2006 (Cambridge, MA) 26-28 June 2006.

30. Camp, L.J & Yee, K-P (2003). Human implications of technology. Practical Handbook of Internet Computing ed. M. P. Singh, CRC Press (New York, NY) Winter 2003.

31. Camp, L.J (2003). Peer to Peer Systems, The Internet Encyclopedia ed. Hossein Bidgoli, John Wiley & Sons (Hoboken, New Jersey) 2003.

32. Camp, L.J (2003). Design for Trust, Trust, in Reputation and Security: Theories and Practice, ed. Rino Falcone, Springer-Verlang (Berlin) 2003.

33. Camp, L.J & Osorio, C (2003). Privacy Enhancing Technologies for Internet Commerce, Trust in the Network Economy, Springer-Verlag (Berlin) 2003.

34. Camp, L.J, McGrath, C & Nissenbaum, H (2001). Trust: A Collision of Paradigms, Proceedings of Financial Cryptography, Lecture Notes in Computer Science, Springer-Verlag (Berlin, Germany) Fall 2001.

35. Cardholm, L (1999). Building Trust in an Electronic Environment, in *Proceedings of the Fourth Nordic Workshop on Secure IT Systems (Nordsec '99)*, November 1-2, 1999, Kista, Sweden, pp. 5-20

36. Cardoso C, Keates S, Clarkson PJ (2002). Designing for Inclusivity - Assessing the accessibility of everyday products. In the *Proceedings of CWUAAT '02*, Springer.

37. Cassell, J. and Bickmore, T (2000). External Manifestations of Trustworthiness in the Interface". *Communications of the ACM*, December 2000, Vol. 43, No. 12, pp. 50-56

38. Castelfranchi C. (2004). Formalising the informal? Dynamic social order, bottom-up social control, and spontaneous normative relationsm *Journal of Applied Logic*, Volume 1, Issue 1-2 (February 2003), pp. 47-92

39. Castelfranchi C., Falcone R., Marzo F. (2006). Being Trusted in a Social Network: Trust as Relational Capital. *Lecture Notes on Artificial Intelligence (LNAI)*, Springer

40. Cheskin (1999). ECommerce Trust Study. January 12, 1999. Cheskin Research and Studio Archetype/Sapient. 31. http://www.cheskin.com/cms/files/i/articles//17__report-eComm%20Trust1999.pdf

41. Cheskin (2000). Trust in the Wired Americas. Cheskin Research July 2000. http://www.cheskin.com/assets/report-CheskinTrustIIrpt2000.pdf

42. Chong, B., Yang, Z., Wong, M (2003). Asymmetrical Impact of Trustworthiness Attributes on Trust, Perceived Value and Purchase Intention: A Conceptual Framework for Cross-cultural Study on Consumer Perception of Online Auction, in Proceedings of ICEC 2003, Pittsburgh, PA. ACM Press, pp. 213-219.

43. Chu, Y-H. et al (1997). REFEREE: Trust Management for Web Applications, *World Wide Web Journal*, 2

44. Clarke, R (1999). Internet Privacy Concerns Confirm the Case for Intervention, *Communications of the ACM*, Vol. 42, No. 2, February 1999, pp. 60-67

45. Cranor, L.F, Garfinkel, S (eds.) (2005). Security and Usability: Designing Secure Systems that People Can Use. O'Reilly.

46. Cranor, L.F, Reagle, J. and Ackerman, M. S. (1999). Beyond Concern: Understanding Net Users' Attitudes about On-line Privacy. *AT&T Labs-Research Technical Report TR 99.4.3*, http://www.research.att.com/library/trs/TRs/99/99.4/

47. Cranor, L.F., Guduru, P, Arjula, M. (2006). User Interfaces for Privacy Agents. ACM Transactions on Computer-Human Interaction 13(2) , June 2006, 135-178

48. Cranor, L.F., Zhang, Y., Hong, J. (2007). CANTINA: A Content-Based Approach to Detecting Phishing Web Sites. In Proceedings of the 16th International World Wide Web Conference (WWW2007), Banff, Alberta, Canada, May 8-12

49. Cyr, D., Head, M. and Ivanov, A. (2006). Design Aesthetics Leading to M-loyalty in Mobile Commerce. Information and Management.

50. DeWitt, A. J. and Kuljis, J. (2006). Is usable security an oxymoron?. interactions 13, 3 (May. 2006), 41-44

51. Dhamija, R (2000). Hash Visualization in User Authentication, in *Proceedings of CHI '2000*, The Hague, Amsterdam, ACM Press, pp. 279-280

52. Dhamija, R., Tygar, J.D., Hearst, M (2006). Why Phishing Works. In Proceedings of the SIGCHI conference on Human factors in computing systems (CHI'06), ACM Press

53. Diller, S., Lin, L., and Tashjian, V (Cheskin) (2002). The Evolving Role of Security, Privacy and Trust in a Digitized World, in The Human-Computer Interaction Handbook - Fundamentals, Evolving Technologies, and Emerging Applications, Julie A. Jacko (ed.) and Andrew Sears (ed.) Copyright 2002 Lawrence Erlbaum Associates, Inc.

54. Donath, J.,Boyd, D. (2004). Public Displays of Connection BT Technology Journal Vol 22 No 4. October 71-82

55. Dourish, P, Grinter, R.E, Delgado de la Flor, J, Joseph, M (2004). Security in the wild: user strategies for managing security as an everyday, practical problem. In *Personal and Ubiquitous Computing* (2004) 8: 391-401

56. Egger, F. N.(2001). Affective design of e-commerce user interface: How to maximize perceived trustworthiness. In Proceedings of the International Conference on Affective Human Factors Design. London: Academic Press.

57. Egger, F.N. (2003). From Interactions to Transactions: Designing the Trust Experience for Business-to-Consumer Electronic Commerce. PhD Thesis, Eindhoven University of Technology (The Netherlands)

58. Ellison, C (2002). Home Network Security. *Intel Technology Journal, interoperable Home Infrastructure*, Volume 6, Issue 4, November 15, 2002, pp. 36-48. Availble: http://developer.intel.com/technology/itj/index.htm

59. EPIC 2005. Privacy Self Regulation: A Decade of Disappointment, by Chris Jay Hoofnagle, March 4, 2005, http://www.epic.org/reports/decadedisappoint.html

60. Endres-Niggemeyer, B (1999). Grounded theory methodology for knowledge engineering. IJCAI99, Stockholm, 31 July - 6 August 1999, Workshop "Empirical AI".

61. Eronen, P, Lehtinen, J, Zitting, J, Nikander P (2000). Extending Jini with Decentralized Trust Management, in *Proceedings of OpenArch'2000*, Tel Aviv, Israel.

62. Fagin, R, Halpern, J.Y (1988). I'm ok if you're ok: on the notion of trusting communication, *Journal of Philosophical Logic*, 17:4, pp. 329-354, Nov.

63. Falcone, R and Castelfranchi, C (2001). The Socio-Cognitive Dynamics of Trust: Does Trust Create Trust? *in* R. Falcone, M. Singh, and Y.-H. Tan: Trust in Cyber-societies, LNAI 2246, pp. 55–72, 2001. Springer-Verlag Berlin Heidelberg

64. Feng, J., Lazar, J. and Preece, J (2003). Interpersonal Trust and Empathy Online: A Fragile Relationship, in Proceedings of CHI 2003, New Horizons, April 5-10, Fort Lauderdale, Florida USA. ACM Press, pp. 718-719.

65. Ferscha, A, Hechinger, M, Mayrhofer, R, Chtcherbina, E, Franz, M, dos Santos Rocha, M and Zeidler, A (2005). Bridging the gap with P2P patterns. In *Proceedings of the Workshop on Smart Object Systems*, September 2005. in conjunction with the Seventh International Conference on Ubiquitous Computing (UbiComp 2005)

66. Flechais, I., Riegelsberger, J. & Sasse, M.A. (2005). Divide and Conquer: The role of trust and assurance in the design of secure socio-technical systems. Proceedings of the New Security Paradigms Workshop, Lake Arrowhead, California, Sept 20-23

67. Fogg, B.J. et. al.(2000). Elements That Affect Web Credibility: Early Results from a Self-Report Study. *Proceedings of CHI2000*, Short talks.

68. Fogg, B.J. (2003). Persuasive Technology. Using Computers to Change What We Think and Do. Morgan Kaufmann Publishers, San Francisco USA

69. Fogg, B.J., Soohoo, C., Danielson, D.R., Marable, L., Stansford, J., Tauber E.R. (2003). How Do Users Evaluate the Credibility of Web Sites? A Study with Over 2,500 Participants, ACM Press

70. Franco, R. (2005). Better Website Identification and Extended Validation Certificates in IE7 and Other Browsers. http://blogs.msdn.com/ie/archive/2005/11/21/495507.aspx, Nov. 21.

71. Friedman, A & Camp, L.J, (2004). Security in Peer to Peer Systems, The Handbook of Information Security ed. Hossein Bidgoli, John Wiley & Sons (Hoboken, New Jersey)

72. Friedman, B, Kahn P.H Jr and Howe, D.C. (2000), Trust Online. *Communications of the ACM*, December 2000, Vol. 43, No. 12, pp. 34-40

73. Fukuyama, F (1995). Trust: The Social Virtues and the Creation of Prosperity, Free Press

74. Ganesan, S (1994). Determinants of Long-Term Orientation in Buyer-Seller Relationships, Journal of Marketing, Vol. 58, No. April, pp. 1-19.

75. Gefen, D. (2002). Reflections on the Dimensions of Trust and Trustworthiness among Online Consumers. ACM SIGMIS Database, Vol 33, issue 3 Summer 2002, ACM Press New York, USA pp. 38-53.

76. Gefen, D., Rao, V.S., Tractinsky, N (2002). The Conceptualization of Trust, Risk and Their Relationship in Electronic Commerce: The Need for Clarifications. 36th Hawaii International Conference on Systems Sciences

77. Gelbord, B (2000). Signing Your 011001010. The problems of digital signatures. *Communications of the ACM*, December 2000, Vol. 43, No. 12, pp. 27-28

78. Giddens, A (1989). Consequences of Modernity, Stanford: Stanford University Press

79. Glaser, B.G, Strauss, A.L. (1967/1980). The Discovery of grounded theory: Strategies for qualitative research (11th ed.). New York: Aldine Atherton.

80. Good, N.S. and Kreckelberg, A (2003). Usability and privacy: a study of KaZaA P2P file-sharing. CHI 2003, April 5-10, 2003, Ft. Lauderdale, Florida USA. ACM Press

81. Grandison, T and Sloman, M. (2000). A Survey of Trust in Internet Applications. IEEE Communications Surveys, The Electronic Magazine of Original Peer-Reviewed Survey Articles. Fourth Quarter 2000, pp. 2-12. http://www.comsoc.org/pubs/surveys

82. Grinter, R.E, Edwards, W.K, Newmann, M.W, Ducheneaut, N (2005). The Work to Make a Home Network Work. In H. Gellersen, H (eds), ECSCW 2005: *Proceedings of the Ninth European Conference on Computer-Supported Cooperative Work*, 18-22 September 2005, Paris, France, pp.469-488. Springer, Netherlands

83. Hart, P and Liu, Z (2003). Trust in the Preservation of Digital Information, in Communications of the ACM, June 2003/Vol. 46, No. 6, pp. 93-97.

84. Hartman, S. (2006). IETF Internet-Draft: Requirements for Web Authentication Resistant to Phishing. http://www.ietf.org/internet-drafts/draft-hartman-webauthphishing-02.txt, Oct. 21.

85. Hawkins, W.H (1999). Designing Effective Multilingual Voice Services, in *Proceedings of 17th International Symposium, Human Factors in telecommunications 1999*, Copenhagen, Denmark, pp. 59-64

86. Hawthorn, D (2000). Possible Implications of Aging for Interface Designers, *in Interacting with Computers*, Vol. 12 (5), Elsevier Science, B.V., 2000, pp. 507-528

87. Hoffman, D.L, Novak, T.P, Peralta, M (1999). Building Consumer Trust On-line, *Communications of the ACM*, April 1999, Vol. 42, No. 4, pp. 80-85

88. Holmström, U (1999). User-Centred Design of Security of Software, *in Proceedings of 17th International Symposium, Human Factors in Telecommunications 1999*, Copenhagen, Denmark, pp. 49-57

89. Hwang, F, Keates S, Langdon P, Clarkson PJ, Robinson P (2002). Cursor characterisation and haptic interfaces for motion-impaired users. *Universal Access and Assistive Technology*, Springer-Verlag (eds. Keates, Clarkson, Langdon, Robinson)

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

91. Jarvenpaa, S.L., Tractinsky, N., Vitale, M. (2000). Consumer Trust in an Internet Store, Information Technology and Management , 1(1-2): 45-71

92. Jensen, C, Farnham S.D, Drucker, S.M, Kollock, P (2000). The Effect of Communication Modality on Cooperation in Online Environments, in *Proceedings of the CHI 2000*, ACM, New York, pp. 470-477. The Hague, Netherlands, April 1-5. ACM Press.

93. Jordan, P. W.(2000). Designing pleasurable products. An introduction to the New Human Factors. Taylor & Francis

94. Jøsang, A (1998). Modelling Trust in Information Society, Ph.D. Thesis, Department of Telematics, Norwegian University of Science and Technology, Trondheim, Norway

95. Jøsang, A (1999). Trust-based decision making for electronic transactions, in L.Yngström and T.Svensson (Eds.) *Proceedings of the Fourth Nordic Workshop on Secure IT Systems (NORDSEC'99),* Stockholm, Sweden, Stockholm University Report 99-005, 1999.

96. Jøsang, A, Patton, M.A, Ho, A (2001). Authentication for Humans, in Proceedings of the 9th International Conference on Telecommunication Systems (ICTS2001), Dallas.

97. Karvonen, K (2007). Users and Trust: the New Threats, the New Possibilities, (invited paper), to appear in Proceedings of 4th International Conference on Universal Access in Human-Computer Interaction, 22-27.7.2007, Beijing, China, Springer-Verlag LNCS

98. Karvonen, K, Kortesniemi Y, Latva-Koivisto A (2001). Evaluating Revocation Management in SPKI from a User's Point of View, in the *Proceedings of the 18th International Symposium on Human Factors in Telecommunications (HfT'01),* November 5-7, 2001, Bergen, Norway

99. Karvonen, K, Parkkinen, J (2004). User Interfaces and Usability in Multi-Channel Products, in Korpiaho, M. (ed.): Multi-Channel Solutions: Content, Technology, Concepts and Usage, Addison Wesley, pp. 105-132

100. Keates S, Clarkson PJ, Robinson P (2002). Developing a practical inclusive interface design approach, *Interacting with Computers*, Elsevier, Vol. 14, No 4, July 2002, pp 271-299.

101. Keats, D.M (2000). Interviewing. A practical guide for students and professionals, Open University Press, Buckingham, Philadelphia

102. Kelvin, P. (1973). A Social Psychological Examination of Privacy. *British Journal of Social and Clinical Psychology*, 12, 248-261.

103. Ketelaar, E (1997). Can We Trust Information?, in *International Information & Library Review*, Academic Press Limited, 1997, 29, pp. 333-338

104. Kim, D.J, Ferrin, D.L., Rao, H.R (2003). A study of the Effect of Consumer Trust on Consumer Expectations and Satisfaction: the Korean Experience. ICEC 2003, Pittsburgh, PA, pp. 310- 315

105. Kim, J, Lee, J Choi, D (2003). Designing emotionally evocative homepages: an empirical study of the quantitative relations between design factors and emotional dimensions, International Journal of Human-Computer Studies, v.59 n.6, p.899-940, December 2003

106. Kopala, M, Suzuki, L.A (Eds.) (1999). Using Qualitative Methods in Psychology, Sage Publications, Thousand Oaks, U.S.

107. Landauer, T.K. (1997). Behavioral Research Methods in Human-Computer Interaction. In Helander, M, Landauer, T.K, Prabhu P (eds.), Handbook of Human-Computer Interaction, 2nd, revised ed. Elsevier Science B.V, Amsterdam, pp. 203-228

108. Lau, T, Etzioni, O, Weld, D.S (1999). Privacy Interfaces for Information Management, *Communications of the ACM*, Vol. 42, No. 10, October 1999, pp. 89-94

109. Lavie, T. and Tractinsky, N. (2004). Assessing Dimensions of Perceived Visual Aesthetics of Web Sites, International Journal of Human-Computer Studies, 60(3):269-298.

110. Lehti, I, Nikander, P (1998). Certifying trust, in *Proceedings of the Practice and Theory in Public Key Cryptography (PKC) '98*, Yokohama, Japan, Springer-Verlag, February 1998.

111. Lewis, D. and Weigert, A.J (1985a). Social Atomism, Holism, and Trust, *in The Sociological Quarterly* 26, no.4 (1985), pp. 455-71

112. Lewis, D. and Weigert, A.J (1985b). Trust as Social Reality, in *Social Forces* 63, no. 4 (June 1985)

113. Liimatainen, S (2005). Usability of Decentralized Authorization Systems - A Comparative Study, Proceedings of the 38th Annual Hawaii International Conference on System Sciences (HICSS'05)

114. Lindgaard, G, Fernandes, G, Dudek, C, Brown, J (2006). Attention web designers: You have 50 milliseconds to make a good first impression! In Behaviour & Information Technology, Vol. 25, No. 2, March-April 2006, 115-126

115. Litman, J (2000). Information Privacy/Information Property, 52 *Stanford L. Rev*. 1283

116. Loukola, O (1999). Who Do You Trust? Combining Morality and Rationality" Diss, University of Helsinki, Acta Philosophiceae, No 4, Tammavuoren Kirjapaino Oy, Vantaa

117. Luhmann, N (1979). "Trust: A Mechanism For the Reduction of Social Complexity." Trust and Power: Two works by Niklas Luhmann. New York: John Wiley & Sons

118. Luo, W., Najdawi, M. (2004). Trust-building measures: a review of consumer health portals, in Communications of the ACM, Vol 47, No 1 (2004) pp. 108-113

119. Masten, D, Plowman, T (2003). Digital ethnography: The next wave in understanding the consumer experience. Design Management Journal, Vol. 14, No. 2, Spring 2003, pp. 75-81

120. Millar, R., Crute, V. and Hargie, O. (1992). Professional Interviewing, Routledge, London

121. Mitnick, K. D. & Simon, W. L, Wozniak, S. (2002). The Art of Deception: Controlling the Human Element of Security. Wiley Publishing Inc

122. Mühlfelder, M, Klein, U, Simon, S, Luczak, H (1999). Teams without Trust? Investigations in the Influence of Video-Mediated Communication on the Origin of Trust

among Cooperating Persons, in *Behaviour & Information Technology*, Vol. 18, No. 5, 1999, pp. 349-360

123. Nielsen, J. (1993). Usability Engineering, Academic Press, Boston.

124. Nielsen, J. (1999a). Trust or Bust: Communicating Trustworthiness in Web Design, *Alertbox*, March 7, 1999, at http://www.useit.com/alertbox/990307.htm

125. Nielsen, J. (1999b). Why you only need to test with 5 users, Jacob Nielsen's Alertbox, March 19, 1999 http://www.useit.com/alertbox/20000319.htm

126. Nielsen, M., Krukow, K (2003). Towards a Formal Notion of Trust, in Proceedings of PPDP '03, August 27-29, Uppsala, Sweden, ACM Press, pp. 4-7

127. Nielsen Norman Group (2001). E-commerce User Experience. Design Guidelines for Trust and Credibility

128. Nikander, P (1999). An Architecture for Authorization and Delegation in Distributed Object-Oriented Agent Systems, PhD. Thesis, Helsinki University of Technology, March.

129. Nikander, P (1997). Modelling of Cryptographic Protocols, Licenciate's Thesis, Helsinki University of Technology, December.

130. Norman, D. (2004). Emotional Design: Why We Love (Or Hate) Everyday Things. Basic Books

131. Norman, D (1986). The Design of Every-Day Things, London. MIT, 1986/1998

132. Olson, J.S and Olson G.M. (2000). i2i Trust in E-Commerce, *in Communications of the ACM*, December 2000, Vol. 43, No. 12, pp. 41-44

133. Pedersen, D.M. (1997). Psychological Functions of Privacy. *Journal of Environmental Psychology*, 17, 147-156

134. PGP Users Guide, Chapter 1: How PGP works, http://www.pgpi.org/doc/pgpintro/

135. Picard, R.W. (1997). Affective computing, MIT Press, Cambridge, MA

136. Princeton Survey Research Associates (2005). Leap of Faith. Using the Internet Despite the Dangers. Results of a National Survey of Internet Users for Consumer WebWatch. www.consumerwebwatch.org/pdfs/princeton.pdf

137. Princeton Survey Research Associates (2002). A Matter of Trust: What Users Want From Web Sites. Results of a National Survey of Internet Users for Consumer WebWatch. http://www.consumerwebwatch.org/news/report1.pdf

138. Privacy Online (1998). A Report to Congress, Federal Trade Commission, June 1998, http://www.ftc.gov/reports/privacy3/index.htm

139. Riegelsberger, J (2003). Interpersonal Cues and Consumer Trust in E-Commerce. CHI 2003 New Horizons, Doctoral Consortium, April 5-10, Fort Lauderdale, Florida USA. ACM Press, pp. 674-675.

140. Riegelsberger, J & Sasse, M.A (2002). Face It: photos of staff don't make a web-site trustworthy. To be presented as a Short Talk at CHI 2002, Minneapolis, April 20-25, pp. 742-743

141. Riegelsberger, J., Sasse, M.A., & McCarthy, J (2002). Eye-catcher or blind spot? The effect of photographs of faces on e-commerce web sites. In J. L. Monteiro, P. M. C. Swatman & L. Valaderes Tavares: Towards the Knowledge Society - eCommerce, eBusiness and eGovernment. Proceedings 2nd IFIP Conference on e-commerce, e-business, e-government (I3E), Oct 7-9, Lisbon, Portugal, pp. 383-398.

142. Riegelsberger, J., Sasse, M.A., & McCarthy, J (2003). Shiny Happy People Building Trust? Photos on e-Commerce Websites and Consumer Trust. Proceedings of CHI 2003, Ft. Lauderdale, Florida, April 5-10, 2003, pp. 121-128

143. Riegelsberger, J., Sasse, M.A., & McCarthy, J (2003). The Researcher's Dilemma: Evaluating Trust in Computer Mediated Communications. International Journal of Human Computer Studies, Vol. 58, 759-781.

144. Riegelsberger, J & Sasse, M.A (2001). Trustbuilders and trustbusters: The role of trust cues in interfaces to e-commerce applications, in B. Schmid, K. Stanoevska-Slabeva & V. Tschammer: *Towards the E-Society: Proceedings of the 1st IFIP Conference on e-commerce, e-business, e-government*, Oct. 3-5 2001. pp. 17-30. Kluwer.

145. Riegelsberger J. Vasalou A., Bonhard P., Adams A. (2006). Reinventing Trust, Collaboration, and Compliance in Social Systems, Extended Abstracts of CHI 2006, Montréal, Canada, ACM Press

146. Rocco, E (1998). Trust Breaks Down in Electronic Contexts but Can Be Repaired by Some Initial Face-to-Face Contact, in *Proceedings of CHI '98*, April 18-23, 1998, Los Angeles, CA.

147. Rosenbloom, A (2000). Trusting Technology. *Communications of the ACM*, December 2000, Vol. 43, No. 12, pp. 31-32

148. Rousseau, J-J (1762/1987). The Social Contract, Reprint edition, tranlated by Maurice Cranston, September 1987, Penguin Books, USA.

149. Rubin H.J. and Rubin I.S. (1995). Qualitative Interviewing. The Art of Hearing Data. Sage Publications, Thousand Oaks, U.S.

150. Saariluoma, P (2004). Käyttäjäpsykologia. Ihmisen ja koneen vuorovaikutuksen uusi ajattelutapa. WSOY Helsinki

151. Safer Internet (2006). Eurobarometer survey on Safer Internet, http://europa.eu.int/information_society/activities/sip/docs/eurobarometer/eurobarometer_2005_25_ms.pdf

152. Salam, A.F, Rao, H.R., and Pegels, C.C. (2003). Consumer-Perceived Risk in E-Commerce Transactions, in Communications of The ACM, December 2003/Vol. 46, No. 12 ve, pp. 325-331

153. Sandhu, R (2003). Good-Enough Security: Toward a Pragmatic Business-Driven Discipline, *IEEE Internet Computing*, vol. 07, no. 1, pp. 66-68, Jan/Feb, 2003.

154. Sasse, M.A. (2003). Computer Security: Anatomy of a Usability Disaster, and a Plan for Recovery. Paper presented at the CHI 2003 Workshop on Human-Computer Interaction and Security Systems, Ft. Lauderdale, April 5

155. Sasse, M.A (2005). Usability and Trust in Information Systems. In: Trust and Crime in Information Societies, edited by Robin Mansell and Brian S Collins, pp. 319-348. Edward Elgar. ISBN 1 84542 177 9

156. Sasse, M.A. & Flechais, I (2005). Usable Security: What is it? How do we get it? In: Cranor, L.F & Garfinkel, S (Eds.): Security and Usability: Designing secure systems that people can use. pp. 13-30. O'Reilly Books

157. Schechter, S., Dhamija, R., Ozment, A., Fischer, I. (2007). The Emperor's New Security Indicators, to appear in the Proceedings of the IEEE Symposium on Security and Privacy, May 2007

158. Schechter, S, Greenstadt, R, and Smith, M (2003). Trusted Computing, Peer-to-Peer Distribution, and the Economics of Pirated Entertainment, *Proceedings of the 2nd Inernational Workshop on Economics and Information Security*, 2003; www.eecs.harvard.edu/%7Estuart/papers/eis03.pdf

159. Seligman, A.B (1997). The Problem of Trust, Princeton University Press, New Jersey.

160. Shneiderman, B (2000). Designing Trust into Online Experiences. *Communications of the ACM*, December 2000, Vol. 43, No. 12, pp. 57-59

161. Shneier, B (2000). Secrets and Lies. Digital Security in a Networked World. John Wiley & Sons, USA

162. Simmons, G.J (1993). An introduction to the mathematics of trust in security protocols, in *Proc. Computer Security Foundations Workshop IV*, pp. 121-127, Franconia, N.H., 15–17 June, IEEE Computer Society Press, Los Alamitos, CA.

163. Simmons, G.J, Meadows, C.A (1994). The Role of trust in information integrity protocols, *Journal of Computer Security*, 3:2

164. Spinellis, D (2003). Reflections on Trust. Trust Revisited. Communications of the ACM, June 2003, Vol. 46 No. 6, p.112

165. Stewart, K.J (2003). Trust Transfer on the World Wide Web, in Organization Science 14(1): 5-17.

166. Stewart, K.J, Zhang, Y (2003). Effects of Hypertext Links on Trust Transfer, in Proceedings of ICEC 2003, Pittsburgh, PA, ACM, pp. 235-239.

167. Strauss, A., Corbin, J., (1998). Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory, 2nd Edition. Sage, Newbury Park

168. Surendra N. Singh , Nikunj P. Dalal, (1999). Web home pages as advertisements, Communications of the ACM, v.42 n.8, p.91-98, Aug. 1999

169. Surfer Beware III (1999). Privacy Policies without Privacy Protection, Electronic Privacy Information Center, December 1999, http://www.epic.org/reports/surfer-beware3.html

170. Syverson, P, van Oorschot, P.C (1994). On unifying some cryptographic protocol logics, in *Proc. 1994 IEEE Computer Society Symposium on Research in Security and Privacy*, pp. 14-28

171. Tang, F-F., Thom, M.G., Wang, L.T., Tan, J.C., Chow, W.Y and Tang, X (2003). Using Insurance to Create Trust on the Internet, in Communications of the ACM, December 2003/Vol 46, No. 12 ve, pp. 337-344.

172. Taviani, H.T. (1996). Computer Matching and Personal Privacy: Can They Be Compatible? In *Proceedings of CQL '96*, Philadelphia PA, USA, pp. 97-101

173. Teltzrow, M., Günther, O., Pohle, C (2003). Analyzing Consumer Behavior at Retailers with Hybrid Distribution Channels - A Trust Perspective, in Proceeding of ICEC 2003, Pittsburgh, PA, ACM Press, pp. 422-428

174. Tractinsky, N. (1997). Aesthetics and Apparent Usability: Empirically Assessing Cultural and Methodological Issues, CHI 97 Conference Proceedings, Atlanta, March 22-27, 1997), ACM, New York, pp. 115-122

175. Tractinsky, N., Katz, AS, and Ikar, D (2000). What is beautiful is usable, in Interacting with Computers, 13 (2000), 127-145

176. Uzun, E, Karvonen, K, Asokan, N (2007). Usability Analysis of Secure Pairing Methods, in Proceedings of Usable Security (USEC'07), February 15-16, 2007, Trinidad&Tobago, a workshop co-located with The Eleventh Conference on Financial Cryptography and Data Security (FC'07)

177. Wang, H., Lee, M.K.O. & Wang, C. (1998). Consumer Privacy Concerns about Internet Marketing. *Communications of the ACM*, 41(3), 63-70.

178. Wang, Y.D, Emurian, H.H (2005). Trust in E-Commerce: Consideration of Interface Design Factors, Journal of Electronic Commerce in Organizations, 3(4), 42-60, October-December 2005

179. Weippl, E and Essmayr, W (2003). Personal Trusted Devices for Web Services: Revisiting Multilevel Security, in Mobile Networks and Applications 8, 151-157, 2003, Kluwer Academic Publishers, Netherlands.

180. White, G.B, Fisch, E.A, Pooch, U.W (1996). Computer Systems and Network Security, CRC Press 1996.

181. Whitten, A, Tygar, J.D (1998). Usability of Security: A Case Study, Carnegie Mellon School of Computer Science Technical Report, December 1998

182. Whitten, A, Tygar, J.D (1999). Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0, in *Proceedings of the 8th USENIX Security Symposium*, August 1999.

183. Wilhelm, G.U, Staamann, S, Buttyán, L (1998). On the Problem of Trust in Mobile Agent Systems, in *Proceedings of the 1998 Network And Distributed System Secu-rity Symposium*, March 11-13, 1998, San Diego, California, Internet Society.

184. Yahalom, R, Klein, B, Beth, T (1993). Trust relationships in secure systems: a distributed authentication perspective, in *Proceedings of 1993 IEEE Computer Society*

Symposium on Research in Security and Privacy, pp. 150-164, IEEE Computer Society Press, May 1993.

185. Yahalom, R, Klein, B, Beth, T (1994). Trust-based navigation in distributed systems, *Computing Systems*, 7:1, pp. 45-73.

186. Yang, Y, Hu, Y, Chen, J (2005). A web trust-inducing model for e-commerce and empirical research, in the Proceedings of 7th international conference on Electronic commerce (ICEC'05), August 15-17, 2005, Xi'an, China, ACM Press, pp. 188-194.

187. Yee, K-P. (2005). Guidelines and Strategies for Secure Interaction Design, in Cranor, L.F & Garfinkel, S (Eds.): Security and Usability: Designing secure systems that people can use. O'Reilly Books 247-274

188. Yolum, P. and Singh, M.P: Ladders of Success (2003). An Empirical Approach to Trust. In proceedings of AAMAS'03, July 14-18, 2003, Melbourne, Australia, pp. 1168-69

189. Zhang, X, Chen, S, and Sandhu, R (2005). Enhancing Data Authenticity and Integrity in P2P Systems, IEEE Internet Computing, Special Issue on Security for P2P/Ad Hoc Networks, 9(6): 42-49, November 2005

8 Appendix: User interview structure

8.1 General questions

The semi-structured interviews contained questions to establish the user's general experiences and thoughts of online shopping. The questions were divided into eight groups.

User study on Trust functions				Date:		Ref.No:
1 Background						
1.1 Sex:	(M) (F)	1.2 Age:	yrs	1.3 Education:		
2 Use experience						
2.1 Computers, money card (cash card), credit cards, bank cards, other cards						
2.2 Automats: cash machine (ATM), ticket automat						
2.3 The web: For how long has the user been using the Web? How often?						
2.4 Ecommerce (as a consumer)						
2.5 Electronic library services						
2.6 Does the user have a home page? If yes, what kind of information is there?						
2.7 Email: does the user use email, which post service/program does she use?						
2.8 Other information the user might want to add						
3 Differences between different means of payment						
3.1 What, in your opinion, are the most significant differences between different means of payment? For example, when would you rather use credit card than cash or the other way round?						
3.2 What is the difference between bankcard and credit card? Do you use them differently?						
3.3 What is the difference between money card (cash card) and bankcard?						
3.4 What kind of cards are you normally using						
3.4.1 Why did you choose these?						
3.4.2 Are there some deficiencies in these that you have noticed?						
3.4.3 Are there some features missing that you would like to have?						
3.4.4 Have you ever had any trouble using these means of payments? If yes, what kind?						
3.5 What about automats (ATM)? Have you ever had trouble with them?						
3.6 What means of payment do you use when travelling? Why?						

4 Internet banking and online services of banks	
4.1 Do you use the online services of your bank? If yes, where and when?	(Yes) (No)
At: (Home) (Work)	Other and when:
4.1.1 How did you start using these services?	
4.1.2 What was the motivator?	
4.1.3 Did someone help you with it?	
4.1.4 How did you find out about the online services?	
4.1.5 Do you friends/relatives/work colleagues use these services?	
4.1.6 Do you trust the online services of your bank? Why? Why not?	
4.1.7 Have you, or anyone you know, had any trouble with these services?	
4.1.8 Do you have any ideas of how to make these services better? Are there some features you are missing on the service?	
4.2 Do you trust your bank? Why? Why not?	
4.3 Is your bank domestic or foreign? Does it make any difference to you what the nationality of your bank is?	
(Domestic) (Foreign) (Makes a difference) (Makes no difference)	
5 Ecommerce	
5.1 Have you ever done any business online?	(Yes) (No)
5.2 If YES, do you remember what it was like?	
5.2.1 Which services did you use?	
5.2.2 Do you have some favourites?	
5.2.3 Are your experiences good or bad?	
(Good) (Bad) (Mixed)	
5.2.4 How did you pay for your purchases?	
5.3 If NO, why do you think you have not used any of these services?	
5.4 Do you think you might use them in the future?	
5.5. Do your friends/relatives/work colleagues use ecommerce?	
5.5.1 Which services do they use, that you know of?	
5.6 Does it matter to you whether the service provider is domestic or foreign? Why?	

5.7 What do you think of giving information about yourself on the Web? Would you welcome email with special offers from the service you have used, for example?
6 Email
6.1 What kind of messages do you send? What are they about? To whom?
6.2 Do you write about private matters in your email? What would you consider too private to be written on email?
6.3 Have you ever thought that someone else (a third party) might be going through your email? Do you care?
7 Passwords and log in
7.1 What do you think of the use of passwords in general? Are they a good or a bad way to control access to systems?

7.2 Do you have a password on your computer?	(Yes) (No)

7.3 Is it easy or difficult to remember passwords? Do you have passwords written down somewhere?
7.3.1 What about your credit card/bank card PIN?
7.4 What kind of passwords do you use? Do you use the same password in many places?
7.5 Can you think of a better way to control access than passwords?
8 (Computer) security issues

8.1 Do you ever discuss issues related to computer security with anyone? If yes, where and when?	(Yes) (No)
At: (Home) (Work)	Other and when:

8.2 Do you have knowledge about cases of misuse? For example, have you ever heard about somebody hacking into some system that was considered to be safe?
8.3 Have you read about cases like this in the newspapers/seen in on TV? [Show article]
8.4 Has this kind of information affected your behaviour somehow? For example, have you stopped using some service?
8.5 Has anything like that ever happened to you or someone you know personally? Could you tell more about it?
8.6 How do you get information about security issues? Do you think you are able to get the right information?
8.7 How do you decide whether you can trust some service? What do you base your decision on?
8.8 What about security risks? What kind of security risks do you know of? What should not be done, while, for example, surfing on the Internet? Why/why not?

8.2 Website related questions

The second part of the interviews contained questions to identify the factors of trust most likely to influence the user when deciding whether to trust a service provider or not.

Note: Observations and instructions in brackets ( ). (mark down which category the user chooses)

8.2.1 Basic information

What category is evaluated? _____
and what websites are included in the category?
A)_____
B)_____

What date was the study performed (A) and what is the reference-code (B)?
A)_____
B)_____

You should provide the user with the chance to ask any questions she might have about the user study.

If the user is unfamiliar with any of the sites – start with that one. This gives the interviewer a better chance to see what parts of the site triggers the user's interest or annoyance, which then may be compared to the more familiar site.

Please note which browser (brand and version) is used and if the machine is a PC, Macintosh or other.

Brand, version	Machine
Internet Explorer, ver: ____ Netscape Communicator, ver: ____ Other:_____, ver: ____	(PC) (Mac) (Other:_____)

8.2.2 Questionnaire structure

The questionnaire is divided in six different parts, based on the eCommerce Trust study. The parts are:

1. Presentation
2. Navigation
3. Brand
4. Fulfilment
5. Up-to-date Technology
6. Seals of Approval

The idea is to go through the pages of each service (two services of one category) and discuss the contents and the outlook of the pages at the same time. The interviewer should observe the user's behaviour and make some questions every now and then. Website (A) (repeated for (B))

1 – Presentation

(ask the user to stop on the main page and to give an evaluation of it first and only then ask her to proceed)

Do you find layout of the pages stylish/ unstylish? Why?
(Stylish) (Unstylish)

Are you pleased with the layout? Does it “attract the eye”?
(Yes) (No)

Do you find the pages being outstanding and professional, or rather quite the opposite? Can you say why?
(Professional) (Not professional)

What would you design differently? How would you improve the pages?

2 – Navigation

Is navigation easy? (note: it is better to observe here more than to ask questions)
(Easy) (Difficult)

(Can the user find what she is looking for?) Can you find what you are looking for?
(Easy) (Difficult)

Do you know how to get back to the main page?
(Easy) (Difficult)

Does something annoy you?
(Yes) (No)

Do you have any ideas how to change the structure of the pages?
(Yes) (No)

3 – Brand

Have you *heard* of this service provider before? Where from?
(Yes) (No)

Have you *heard* of this service before? Where from?
Have you seen these pages before?
(Yes) (No)

Have you *used* this service before? Why?
(Yes) (No)

Have you *used* any other services from the service provider? What and why?
(Yes) (No)

Do the pages seem convincing?
(Yes) (No)

Would you consider purchasing something? Why?
(Yes) (No)

4 – Fulfilment

(Does the user seem to know what is going on? Is she surfing in an ordered or in a random way?)
(Ordered) (Random)

Do you get what you want?
(Yes) (No)

Can you cancel the transaction somehow?
(Easy) (Difficult)

Can you find more information about how the pages or the service work?
(Easy) (Difficult)

Is there something that you would like to know but cannot find any information about?
(Yes) (No)

Do you find the pages trustworthy or untrustworthy? Can you say why?
(Trustworthy) (Untrustworthy)

What if there is problem? What can be done?
Can you find any advice on that?
(Easy) (Difficult)

Do you feel treated as an ordinary customer in a “shop on the street” or more like a mail order customer concerning your consumer rights etc? Why?
(Street) (Mail)

5 – Up-to-date Technology

Do you find the pages technology-wise backward or high-tech? What makes you think so?
(High-tech) (Not high-tech)

Do you find the service easy-to-use? Why? Why not?
(Easy) (Difficult)

Are there some technical features missing on the service that you would like to find there?

Which one of the tried webservices in this study do you find the most high-tech?

(Does it seem like the user knows what she is doing? Can she use all the features of the service, e.g. search engines? Does she appear confused? Does she have any problems going through the pages?)

6 – Seals of Approval

Do you know what these are? (*explain if she doesn’t*)
(Yes) (No)

Do you ever remember seeing any ever before, while surfing?
(Yes) (No)

Are there any on these pages?

(Yes) (No) (Easy to find) (Difficult to find) (Not applicable)

Did you notice them before I asked?
(Yes) (No) (Not applicable)

(does the user read the information of the seals on the Net?)
(Yes) (No) (Not applicable)

How do you feel about them? Do they seem trustworthy to you? Why?
(Trustworthy) (Not trustworthy) (Not applicable)

Are there any seals of approval from the real world that you think might fit in here? *(probe: explained if the user does not know what a seal of approval is)*
(Yes) (No)

Finally

The user is asked to discuss the Web services in general, and to compare the two services she just saw (the comparison is, however, not an issue in itself, but might give some insight into why the service appears the way it does to the user).

HELSINKI UNIVERSITY OF TECHNOLOGY
PUBLICATIONS IN TELECOMMUNICATIONS SOFTWARE AND MULTIMEDIA

TML-A1	Håkan Mitts Architectures for wireless ATM	
TML-A2	Pekka Nikander Authorization in agent systems: Theory and practice	
TML-A3	Lauri Savioja Modeling techniques for virtual acoustics	
TML-A4	Teemupekka Virtanen Four views on security	
TML-A5	Tapio Lokki Physically-based auralization – Design, implementation, and evaluation	
TML-A6	Kari Pihkala Extensions to the SMIL multimedia language	print
TML-A7	Kari Pihkala Extensions to the SMIL multimedia language	pdf
TML-A8	Harri Kiljander Evolution and usability of mobile phone interaction styles	
TML-A9	Leena Eronen User centered design of new and novel products: case digital television	
TML-A10	Sanna Liimatainen and Teemupekka Virtanen (eds.) NORDSEC 2004, Proceedings of the Ninth Nordic Workshop on Secure IT Systems	
TML-A11	Timo Aila Efficient algorithms for occlusion culling and shadows	
TML-A12	Pablo Cesar A graphics software architecture for high-end interactive TV terminals	
TML-A13	Samuli Laine Efficient Physically-Based Shadow Algorithms	
TML-A14	Istvan Beszeri Dynamic Layout Adaptation of Web Documents	
TML-A15	Tommi Ilmonen Tools and Experiments in Multimodal Interaction	
TML-A16	Mikko Honkala Web user interaction – a declarative approach based on XForms	
TML-A17	Janne Kontkanen Novel Illumination Algorithms for Off-Line and Real-Time Rendering	
TML-A18	Perttu Hämäläinen Novel Applications of Real-time Audiovisual Signal Processing Technology for Art and Sports Education and Entertainment	