Creating Trust

Kristiina Karvonen

Key words: trust, security, usability, electronic commerce, electronic mail

Abstract:

One of the main problems in the Internet architecture and the applications built on it is the lack of security. This affects the users' willingness to commit any transactions that require providing private information online. The goal of this user study was to find out and analyse the key factors behind users' comprehension of trustworthiness as regards the Web. On basis of conducted user studies a checklist of design features that were found to communicate the trustworthiness of the service to the user was outlined. This list is intended to be used during the design process of a secure user interface that will create trust in the user.

1. INTRODUCTION

The transactions of either money or information on the Web require trust on the users' part. Giving away your credit-card number or providing someone with personal information about yourself is a matter of great sensitivity, and forms a possible threat of this information being misused. This threat can build a barrier for there ever being any transaction of this kind in the first place – if there is no feeling of security, no feeling of

trustworthiness, and the users may restrain themselves from doing business on the Web altogether.

How does the feeling of trust evolve, and how to enhance it? Who should you trust and why? This is an area that has still remained largely untouched by scientific research – until now, there has been only one major study committed on the issue of trust as regards the use of the Internet as a marketplace [1] that we know of. Moreover, the concept of trust is unclear in philosophical, sociological or technical sense also [2].

The purpose of this study was to find out more 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 use of the Web and areas that seemed relevant to this use. These include areas such as use of e-mail, use of bank services, and use of credit cards.

The rest of this paper is organised as follows. In section 2 we define the concept of trust and based on that, motivate the current study. In section 3 there is a description of the user studies that were committed to evaluate the existing research findings as well as to find out more about the users' current ideas about what "trust" is all about. Section 4 analyses the outcome of these interviews. In section 5 the second user interview is presented and analysed. In section 6 we have outlined a design tool for a secure user interface in the form of a checklist of essential design features. Section 7 suggests some focus points for further research. Section 8 presents a conclusion of the conducted study.

2. TRUST

2.1 The Definition of Trust

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" [3] 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 [4].

A sociological study of trust would concentrate more on the distinction between trust in people and trust in "abstract systems". 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 [5]. This trust in "abstract systems", or, a trust in an impersonal, anonymous someone seems to be analogous to the current situation of trust in anonymous service-provider on the Web.

In this study, then, we defined trust as a personal and subjective feeling of trust towards an abstract system that is only partly explicit and rational, and remains partly implicit and irrational. With irrational here is meant that the grounds for the decision-making on trusting or distrusting a system is for the most not explicitly known to the user. The abstract system here is the user interface through which the user has access to the web-based services. This definition of trust formed the starting point for our enquiry, on which the user studies provided more accurate and precise continuation.

2.2 Previous Studies on 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 [6]:

- 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.

In a study conducted at the AT&T Labs [7], implications of a questionnaire on users' attitudes about online privacy 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

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.

The most comprehensive study on trust as regards the Internet so far that we know of is the e-commerce Trust Study committed as a joint research project by Cheskin Research and Studio Archetype/Sapient in January 1999 mentioned earlier [1]. The study was made to find out about the nature of elements behind communicating trust to the user in e-commerce sites, both transactional and graphical. 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 e-commerce trust were considered to be 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

In fact, the 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: all these other studies were using polls 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 motivation for the present study.

In a previous user study in the same project, the user perspective was studied from a more technical point of view, concentrating on the question of just how much the user needs to know about the technical issues behind the user interface in order to be able to make rational choices regarding the security issues [8]. The current study complements that work, but concentrates even more on the user and her actual beliefs.

3. USER INTERVIEWS – A DESCRIPTION

Based on the study of existing literature of the problem area, a set of user interviews was planned. As research method we selected to use ethnographic methods for interviewing the users face-to-face. We also made them have a look on either a mock-up user interface for a movie service online (group 1) or go through some web pages of existing web services (group 2).

The first user interviews 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.

3.1 Users

We chose as our users young academic people because it was thought that they would be most likely to use services online, because they all had computers at their disposal with an easy access to the Internet. We had two groups of users. The first user group consisted of 8 young academic persons, aged 22-30 years, 4 male and 4 female. All had years of experience on using both computers and the Internet, and three of them (all male) could be described as computer professionals – for them, computer was an essential tool in their daily work. The second group also consisted of users with a similar background, aged 23-32, 4 male and 6 female, with 3 males who

were computer professionals. The purpose of having this second set of user interviews was to verify the results of the first interviews.

3.2 First User Group: Testing the Mock-up User Interface for the Movies Service Online

The user interviews were conducted in two phases. First, a simple mock-up user interface was designed to simulate a real service on the Internet[1]. The service was about ordering and watching movies through the Internet, and the users were provided with many alternative ways of paying for their purchases. These included the following: 1) electronic cash, 2) credit card, and 3) bank cheque. As the fourth alternative that was not activated, the users were presented with the idea of an anonymous bank account card that remains anonymous to the merchant, but proves that the holder is authorised to use an account (for more information on this FINEID card see http://www.tcm.hut.fi/Research/TeSSA/HST/index.html).

During the use of the service, the users encountered numerous occasions where more or less private information was inquired from them, such as age, address, education and hobbies. The idea of going through the mock-up service as part of the interview was to evoke questions about the users' willingness to give personal information when the service enquired it. It was also thought that using this service would remind the interviewees of some real-life situations and would thus evoke discussion about those situations and the users' experiences of them.

3.3 Questions Asked

After going through the movie service the users were asked a number of questions covering a wide array of areas that seemed more or less relevant for any considerations of the usability of online security. Banking habits, use of the Internet, use of e-mail and relation to automata were just some of these areas. The questions were loosely grouped around the three key concepts of privacy, security and trust that seemed central to our study. The user habits were investigated in order to find out what it is the user use as their referential mental model when they consider the privacy and security of

[1] This UI was designed by Markku Laukka from the TeSSA project

transactions on the Internet. Is it the habits of using money, or does it have more to do with the routines they have developed while surfing on the Internet or, more specifically, while using e-mail? Or is it something completely different? This origin of the relevant mental model was considered to bear the key to understanding how trust is formed and how it evolves in the users.

Below are some examples of the questions asked from the interviewees:

- What in your opinion are the most significant differences between different means of payment?
- In what situations would you use cash instead of using your credit card?
- Does your bank have an on-line service? If yes, do you use it? Why? Why not?
- Where do you get information on the safety of these services? Do your friends or colleagues use these services?
- Have you purchased anything on the Internet? How willing are you to give personal information about yourself on the Internet? Does it make any difference to you whether the service provider is Finnish or foreign?
- How often do you use e-mail? What mail service do you use? Do you write about sensitive matters in your e-mail? Do you think someone else, a third party, might be observing your mail? Would you care if this were the case?
- How do you feel about using passwords? Is it easy to remember them? Do you have your password written down somewhere?

4. ANALYSIS OF THE USER INTERVIEWS

Next, the user interviews were analysed. The results were loosely grouped along the same lines as the questioning itself.

4.1 Differences between Different Means of Payment

Most users had many different kinds of bankcards and credit cards. Most preferred to use cash or band card for daily purchases and only used credit cards when there was no other choice. This was due to willingness to control the use of money. The users felt that they lose count of their amount of

spending if they use their credit card frequently. The credit card seemed to act as a safety guarantee in case the user ran out of cash or was travelling abroad and suddenly encountered some big expense. Only few of the users had heard about electronic money (such as eCash), and the FINEID card did not interest them much. It was generally felt that the existing paying possibilities were sufficient.

4.2 Electronic Bank Service

Even though the users were not willing to do purchases online, most had tried out the electronic account of their bank online. The users seemed to trust the services provided by their bank. This was so because

- It was felt that banks usually take care of their business well
- The users had never encountered any problems with their bank
- The users were aware that the banks have to follow the law in all their actions and were ready to trust the bank because of this.

To trust the service it seemed to be important that the users had real-life experience of the bank before starting using the electronic service. No one was ready to trust an unknown bank found while surfing on the Net.

Some users had started using the electronic banking services with enthusiasm but had soon given it up. This was because of the clumsiness of the service procedures – they had felt that the system was too complex to be handy. One user felt that he had so few bills that it was no trouble to walk to a cash machine for paying them. It seemed that had the electronic service been easier to use, most users would have continued to use it.

4.3 eCommerce

The user interviews revealed that even though all the users had lots of experience with both computers and Internet and were well aware of the existence of web-based services, they had never actually purchased anything on the Net. The most important reason for this for all users was the lack of trust. The users did not trust that it would be safe to pay with a credit card online. As other reasons the users stated that they did not have the need to buy anything online, or that they would like to be able to touch the merchandise before buying. Some also felt that they might become Net-

Shoppers in the future, once their friends started using the services. Rumours of this kind seemed to be very important for deciding whether use an online-service or not.

Users were reluctant to give information about them when the service enquired for it. This was only partially due to the fear that the information would be maintained by the service provider to create a user profile of them for future marketing purposes. The more important reasons for refusing to give information were more mundane: the users thought they would receive direct marketing mail from the service provider or commit to something, like a membership if they gave away their contact address. The users also felt that it was troublesome to fill in the blank fields.

4.4 E-mail

The users assumed their e-mail account to be private and safe. The users compared e-mail to phone calls considering both to be private. None had ever seriously suspected that someone might be eavesdropping on their e-mail. Yet they were aware that this might be possible, but it was generally felt that the contents of the e-mail was not so personal that it would really be of interest to a third party. The users also wrote sensitive and very personal matters in their e-mail.

4.5 Passwords

Most users found passwords as a good way to secure their privacy. Even though they sometimes forgot their passwords, they did not find this a big problem. The users considered remembering the passwords as everyone's own responsibility. They also used the kind of passwords recommended by the system - partly because the system would not accept any other kind of passwords that would consist of names or words that would be easier to remember. About half of the users used the same password in many places. They also used more easy passwords for services they did not consider so important, such as access to some service on the Internet that required user name and password.

4.6 A Summary of the First User Interviews

The user interviews showed that the users' current understanding of the security of transactions online was imperfect. The decisions about whether to do business online or not were to a great extent based on information gathered from friends, colleagues and newspapers. The users were more ready to trust a service that also existed outside the Net, such as their own bank. In the case of the use of e-mail, the habits of making phone calls and sending regular mail provided a general feeling of trust towards the mail service.

It seemed that once the users started feeling that they really needed a service they were more willing to trade with their trust towards the service. This means they were more ready to use a service even when the trust level was rather low. To give an example, the use of e-mail had become an essential way to stay in contact both in personal and working lives. That is why the users did not really care if their e-mail remained private or not. The need for doing transactions online, however, was not great enough for the users to be ready to trade with their privacy. Many users expressed that they would be interested in using the online services once they have been properly established. They did not want to act as guinea pigs for a new service because it was felt this would be more risky. Once people close to them had started using the existing services successfully, they also would be interested in trying them out.

5. VERIFYING THE RESULTS WITH THE SECOND SET OF USER INTERVIEWS

For the second set of user interviews we decided to replace the mock-up for the movie service with existing web services. Otherwise the questions remained the same, with some questions dropped because they seemed irrelevant to the present study. It was felt that there is a definite need for verifying the results with a second set of user interviews due to the small amount of interviews in the first user study.

5.1 Users

The users were young, aged 23-32, 4 male and 6 female, and had a university degree. Three males could be described as computer professionals. The users went through two existing web services. They could choose one category in four. In each category there were two different shops to go through. The four categories were 1. food markets (www.ruoka.net and www.k-market.com), 2. music shops (www.stupido.fi and www.netinlevy.fi), 3. computer shops (www.pcss.fi and www.24store.index.shtml) and 4. book shops (www.amazon.com and www.bokus.com).

5.2 Questions Asked

Only the questions regarding the existing web pages were new. These questions were made in such a way that they would cover the six primary components found in the eCommerce Trust study to communicate trust (cf. 2.2.).

1. Presentation
- Do you find the layout of the page stylish/unstylish?
- Are you pleased/displeased with the graphics? Does it strike you as professional/unprofessional?
2. Navigation
- Is navigation easy/difficult? Do you find what you are looking for?
- Can you find your way back to the starting page?
- Is there something that annoys you?
- How would you make these pages work?
3. Brand
- Have you heard of the service before, in the Internet or outside it?
- Do you find the service convincing? Would you be ready to purchase something? Why? Why not?
4. Fulfilment
- Do you have a clear picture what is going on?
- Can you find more information about how the service works?
- Do you have questions in mind that remain unanswered?
5. Technology
- Do you find the pages technology-wise advanced or backward? Why?
- Would you expect to find some specific technology on the pages?

- Do you know how to use the pages? Is there anything that is difficult or hard to use?

6. Seals of approval

- Are there any? Did you notice them?
- What do you think of seals of approval? Do you know anything about them?
- Can you find any security information on the pages? Do you find it convincing?

5.3 A Summary of the User Interviews

The interviews proved to verify the results of the first set of interviews, when it comes to the questions regarding the use of different means of payment, e-commerce, e-mail and passwords. Also the observations made by the users about the existing web services were rather similar to those received through the use of the mock-up movie service. The users were eager to evaluate the existing services, but their answers stayed on a very general level and were not specifically trust-oriented. The users were unaware of the existence of any kinds of seals of approval, and when asked about the sense of trust communicated through them, they remained rather suspicious. The users felt that they had no means to evaluate the security of any website.

6. DESIGNING A SECURE USER INTERFACE

Going back to our original research question on how to design a secure user interface that would communicate trustworthiness to the user, a checklist of design features was made on basis of gathered information of the users. This list is intended as an aid for the design of a user interface for any system that is somehow related to the issue of computer security. This all-embracing quality also means that the list is rather general in nature.

6.1 A Checklist for the Designer

Currently, 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. As much as possible should be automatically taken care of on behalf of the user. The user is the weakest link in securing a system. Most security mechanisms are far too difficult for the average user to manage [9]. 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, follow the principles listed below:

- Know your user. Go to the user's environment and talk to her to find out about her level of knowledge regarding technical issues as well as her specific needs and expectations from the system
- Start with listing all the possible security issues embedded in the system
- Automatize as much of the security as possible. The user should be involved with security decisions as little as possible
- Remaining risks should appear as constraints: the user is not allowed to continue working with the system before confirming about the security. However, too much strain is too much. The user must not be prompted about the security too frequently. Instead, the security issues should be taken care of as a whole when user is first introduced to the system
- If possible create a meaningful metaphor through which the user can approach the security issues. Most users are unfamiliar with and afraid of technical issues. Telling her about cryptographic details is of no use and is more likely to decrease the level of trust towards the system than to enhance it

There are really no recognized exemplars of good user interface design for secure user interfaces as yet [9]. The six primary components to promote trustworthiness in the user listed by the eCommerce study [1] are one of the firsts and only kind to even try this. The present study in part verifies 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 this study. It applies to most other components, except for the seals of approval. These were quite unknown to the users, and they were very doubtful about their true value, after they had been told about how these seals should work.

6.2 Quality is Clarity?

Also doubtful remains the component of "presentation" - it only states that quality design connotes professionalism, but what, then, is quality design? This is a question that remains unanswered in the eCommerce study. In the present study 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 straightforward and easy. It is possible, however, that these findings reflect the Finnish user specifically and thus the results cannot be generalized to a more international group of users.

7. SUGGESTIONS FOR FURTHER RESEARCH

7.1 Cultural Differences

It is a well-known fact that besides the individual and social differences between users, differences among users of different cultures are also likely to occur. These differences 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. This point is relevant to any concerns about the usability of computer security, since the Internet is a truly international environment. The culture-specific traits of both the design and the service must be recognised and translated also along the language [10]. It is not enough to change the language of the user interface; the changes must go deeper than that. As important as the language used is the visual outlook and style of the service. 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.

7.2 Groups with Special Needs

Also of interest for future study would be to investigate the needs of groups with specific needs, as regards the feelings of trust, security and privacy. These would include users with different disabilities as well as elderly users (of course, these groups are frequently overlapping).

8. CONCLUSIONS

The purpose of this study was to find out about the formation of trust on the users as regards the use of web-based services. 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 exiting web services to trigger conversation about e-commerce and security issues related to the transactions of money or private information online. The users were questioned 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.

On basis of the user interviews we made a checklist of design qualities that could help to create this trust in the user towards the service. The checklist could then 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 create trust.

Finally, some suggestions for further research topics and focus points were made. These included the study of cultural variation: it was considered likely that there would be a big difference in how users with different cultural background perceive to be trustworthy. The case of users with specific needs - with disabilities or the elderly - was also mentioned. The makings of trust and feeling of trustworthiness was suggested to be different for these special user groups.

9. REFERENCES

[1] eCommerce Trust Study. Joint Research Project by Cheskin Research and Studio Archetype/Sapient. January 1999. http://www.studioarchetype.com/cheskin/)

[2] Seligman, A.B: The Problem of Trust. 1997 Princeton University Press, New Jersey, p. 5-7, 16-17

[3] Lewis, D. and Weigert, A.J: "Trust as Social Reality" in Social Forces 63, no. 4 (June 1985), p. 976

[4] Lewis, D. and Weigert, A.J: "Social Atomism, Holism, and Trust" in The Sociological Quarterly 26, no.4 (1985), pp. 455-71

[5] Giddens, A: Consequences of Modernity, Stanford: Stanford University Press, 1989, p.114

[6] Privacy Online: A Report to Congress, Federal Trade Commission June 1998, http://www.ftc.gov/reports/privacy3/index.htm

[7] Cranor, I.F, Reagle, J. and Ackerman, M.S: Beyond Concern: Understanding net Users' Attitudes About Online Privacy. AT&T Labs-Research Technical Report TR 99.4.3, http://www.research.att.com/library/trs/TRs/99/99.4/99.4/

[8] Holmström, U: User-Centred Design of Security of Software, published in Proceedings of 17th International Symposium, Human Factors in telecommunications 1999, Copenhagen, Denmark, pp. 49-57

[9] Alma Whitten and J.D. Tygar: Usability of Security: A Case Study, Carnegie Mellon School of Computer Science Technical Report, December 1998

[10] The most studied area in the effect of culture-specific elements at the moment is in the multilingual voice services, see e.g. Designing Effective Multilingual Voice Services by W.H.Hawkins from AT&T, published in Proceedings of 17th International Symposium, Human Factors in telecommunications 1999, Copenhagen, Denmark, pp. 59-64