FAKULTÄT FÜR !NFORMATIK

Faculty of Informatics

Guidelines to Support Design and Development of Trust in Mobile Community Applications

DIPLOMARBEIT

zur Erlangung des akademischen Grades

Diplom-Ingenieur

im Rahmen des Studiums

Software Engineering/Internet Computing

eingereicht von

Thomas Wruß
Matrikelnummer 0825404

an der
Fakultät für Informatik der Technischen Universität Wien

Betreuung: Ao.Univ.Prof. Dipl.-Ing. Dr.techn. Peter Purgathofer
Mitwirkung: Univ.Ass. Dipl.-Ing. Eva Ganglbauer

Wien, 06.08.2013

(Unterschrift Verfasser)

(Unterschrift Betreuung)

FAKULTÄT
FÜR !NFORMATIK

Faculty of Informatics

Guidelines to Support Design and Development of Trust in Mobile Community Applications

MASTER'S THESIS

submitted in partial fulfillment of the requirements for the degree of

Diplom-Ingenieur

in

Software Engineering/Internet Computing

by

Thomas Wruß
Registration Number 0825404

to the Faculty of Informatics
at the Vienna University of Technology

Advisor: Ao.Univ.Prof. Dipl.-Ing. Dr.techn. Peter Purgathofer
Assistance: Univ.Ass. Dipl.-Ing. Eva Ganglbauer

Vienna, 06.08.2013

(Signature of Author) (Signature of Advisor)

Technische Universität Wien
A-1040 Wien ▪ Karlsplatz 13 ▪ Tel. +43-1-58801-0 ▪ www.tuwien.ac.at

Erklärung zur Verfassung der Arbeit

Thomas Wruß
Nisselgasse 7, Tür 4, 1140 Wien

Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit - einschließlich Tabellen, Karten und Abbildungen -, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.

(Ort, Datum)	(Unterschrift Verfasser)

Danksagung

Ich möchte mich bei allen bedanken, die mich bei meiner Diplomarbeit unterstützt haben. Ich danke meiner Co-Betreuerin und auch Projektleiterin des Open-Share-It Projektes, Eva Ganglbauer, für die Verbesserungsvorschläge, für das Korrekturlesen und das Beantworten meiner offenen Fragen sowie die tolle Betreuung und Leitung des Open-Share-It Projektes, auch wenn es manchmal unvorhersehbare Wendungen gab.
Ich möchte mich bei Professor Peter Purgathofer bedanken für die gute Zusammenarbeit, seine Ideen und Vorschläge, die erst diese Diplomarbeit ermöglichten und zu dem machte was sie nun ist.
Ich möchte meiner ganzen Familie für die Unterstützung während meiner Studienzeit danken. Besonders meiner Schwester gebührt Dank, da sie sich die Zeit nahm, meine Diplomarbeit Korrektur zu lesen.

Ich danke allen, die die Resultate dieser Diplomarbeit erst ermöglichten, allen InterviewpartnernInnen und den vielen TeilnehmerInnen meiner Umfrage. Erst durch sie konnte ich meine Guidelines vollenden.

Danke!

Abstract

Trust is important for every social network and for most of the mobile applications. However, it is not considered well in many projects and would need more attention.

In this thesis I explore how trust can be generated in community-based mobile applications. In social networks trust plays an important role. Especially in social networks like the Open-Share-It project, which is described in this thesis, trust can be essential for the success of the application. The users do not only have to trust in the social networks and their users, but also in the meetings in real life and the food they share. An important question in this context is how the user's trust in the application can be strengthened. Another important question is how trust between the users can be supported by the application.

I did literature research, carried out interviews and made a survey to explore the creation of trust in such networks. Furthermore, the Open-Share-It project, which has been developed at the Vienna University of Technology, is presented, and its relevance for this thesis is described in more detail. The experiences of this project influence the end results. The results are synthesized in guidelines and compared with the Open-Share-It project. With the guidelines I intend to offer advice about how trust between users can be enhanced by the application and about how the user's trust in the mobile application can be increased.

Kurzfassung

Vertrauen ist in jedem sozialen Netzwerk und für die meisten mobilen Applikationen wichtig. Trotzdem wird Vertrauen oft nicht genügend berücksichtigt und würde mehr Beachtung brauchen.

Diese Diplomarbeit setzt sich mit dem Thema der Vertrauensbildung in sozialen Netzwerken für Smartphones auseinander. Hier spielt Vertrauen eine wichtige Rolle. Gerade in diesen Netzwerken - wie das in der Diplomarbeit vorgestellte Open-Share-It Projekt - kann das Vertrauen für den Erfolg essentiell sein. Die User müssen nicht nur in das Netzwerk und deren Usern Vertrauen haben sondern wollen andere User im realen Leben treffen und Essen austauschen (beziehungsweise übergeben). Eine wichtige Frage in diesem Zusammenhang ist, wie App-Entwickler das Vertrauen der User in die Applikation stärken können. Eine zweite wichtige Frage ist, wie das Vertrauen zwischen Usern durch mobile Applikationen gefördert werden kann.

Für diese Diplomarbeit wurden mittels Recherche, Interviews und einer Umfrage eben solche Netzwerke auf Vertrauensbildung erforscht. Außerdem wird das Open-Share-It Projekt, welches an der Technischen Universität Wien entwickelt wird, in dieser Diplomarbeit vorgestellt und die Zusammenhänge des Projektes mit der Diplomarbeit näher beschrieben. Die Erfahrungen aus diesem Projekt fließen ebenfalls in die Endresultate ein. Die Ergebnisse werden in Guidelines zusammengefasst und im Verlauf der Arbeit auch mit dem Open-Share-It Projekt verglichen. Diese Guidelines sollen Ratschläge geben, wie das Vertrauen zwischen Usern mit der Hilfe von mobilen Applikationen unterstützt werden kann und aufzeigen, wie das Vertrauen eines Users in die mobile Applikation gestärkt werden kann.

Contents

CHAPTER 1

Introduction

In this chapter I introduce the topic of this thesis. In ’Motivation and Problem Statement’ I describe why trust in community-based mobile applications is such an important but also complex topic.

However, hardly any scientific research has been done in this field. Consequently, general guidelines of how to design and develop community-based mobile applications to build up trust do not exist. That is why I decided to develop such guidelines. The goals and the focus of my thesis are defined in ’Aim of the Work’. The methods I use in this thesis are presented in ’Methodological Approach’. In ’State of the Art’ the current situation about smartphones and social networks is described. In ’Additional Information’ I reference Foodsharing and other companies since they play an important role in this thesis and explain the notation for additional information in the thesis. Finally, in ’Structure of the Work’ I describe how this thesis is structured and shortly describe the chapters.

1.1 Motivation and Problem Statement

Trust is important in our daily lives. Everyone has to trust people and objects to fulfil the tasks we want to do. For example: when we buy food, we have to trust the person who cooked it so that it is eatable, when travelling by plane, we have to rely on the pilot or when parents send their children to kindergarten, they have to trust in the kindergarten teacher. So the feeling of trust is something natural that everybody has.

Trust is also important for software development. People often have to trust in different kinds of software. For example, if they use their cellphone, buy something on the Internet or just communicate in a social network. There are many cases when trust is crucial for the user.

But trust is a complex construct and cannot be added with a single mechanism and with a 100% probability. Therefore, trust needs a deeper insight to create software one can trust in. For example, different types of trust have to be considered in software development: the trust between the user and the application and the trust that should be generated between the users through a software application (the first one is called interpersonal trust and the second one institutional trust [WJB08], as I explain in 'Types of Trust') .

Especially in mobile applications trust is very important. A smartphone is often a very personal device. It is usually used by only one person [BBJ11] and stores contacts, photos, e-mails and other private information. These data are sensitive and the user has to rely on the proper use of his/her personal data by the mobile application. Another difference to traditional software development is that smartphones usually have different sensors like GPS. GPS helps you to locate the user. So applications using the GPS sensor know where you are. Therefore, trust should play an important role in mobile application development.

Nowadays, social networks like Facebook[1] or other community platforms are very popular. By using social networks, one can find friends, communicate with others, share information or try to fulfil some task. Especially with smartphones, users can be part of the community any time. Within communities, users have to trust others in many cases: for example, when working together to fulfil some task or even when just sharing some private information.
In other communities, like Foodsharing[2], trust is even more important. With this platform users can share their food that they do not need anymore and some other member of this community can take it for free. So good and edible food is not wasted and dumped, but used and eaten by someone who wants or needs it. In such a community trust is very important: the users have to trust the other users, so that they can meet in real life and then the one who gets the food from the other member has to trust him/her that it is still eatable. Without trust such communities would not work.
However, not all users of social networks trust the system all the time. In a survey M. Faisal and A. Alsumait [FA11] explored that 41% of the participants, who would like to go ahead to share their identity information, think that their identity information is not well-protected against intruders and that their information is used and their actions observed by the owner of the social network.

As one can see, trust should play a far more important role in software development - especially in mobile application development and for community platforms. However, for community-based mobile applications - where trust should be a key element - hardly any research has been done to describe how to design and develop trustful mobile applications.

1.2 Aim of the Work

As I already explained in the 'Motivation and Problem Statement', trust can be crucial for users of different kinds of software. One aim of this thesis is to make the reader aware that trust is an important factor in software development - especially in projects for mobile platforms where people communicate, share information and want to work together in a community. The reader

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

[2] http://www.foodsharing.de

should understand the importance of trust and that trust is very complex and difficult to generate and to maintain.

One aim of this thesis is to develop methods to create more trust between the user and the application in mobile applications and to find out how a mobile application can help to generate trust between users in a community network.

Due to the fact that there has not been done much research in this field, my aim is to introduce guidelines in which the findings are summarized and synthesized. They should help to generate trust between the user and the software as well as between two users with the help of the software. Of course, the guidelines will not guarantee the establishment of trust because trust is very complex and often an individual experience, but they should give the reader some suggestions and remind him/her of the importance of trust in software development.

1.3 Methodological Approach

I will use different approaches to gain new information. First of all, I will do literature research in the field of trust, mobile applications and communities to define and describe these terms. I will also examine mechanisms to generate trust in more detail.

Second of all, I will use qualitative interviews to find new aspects of how trust can be enhanced in community-based mobile applications. These interviews will be constructed like J. F. Gubrium and J. A. Holstein explain in their book [GH02, p. 83]: first preliminary considerations will be done, then the interview itself will take place and at last the data will be interpreted and summarized.
The interviews will be unstructured as it is defined by J. Lazar, J. H. Feng and H. Hochheiser [LFH10, p. 189]. This means that the interviewer starts with a set of questions and topics he/she has prepared beforehand, but may change his/her questions or focus especially on particular questions during the interviews.
The participants of these interviews will be experts in academic areas: people who work at university or students of higher semesters. Since interviews provide deeper and qualitative information, the number of participants is smaller than in a survey [Wei08, p. 3]. The interviews will be face-to-face and will be recorded - if the participant allows me to do so. The information will be analyzed anonymously. A detailed description of the participants, details about the interview, as well as a presentation of the results can be found in the chapter 'Interviews'.

Third of all, I will use a survey to gain information from users about how trust can be improved in community-based mobile applications. According to A. Fink [Fin03a, pp. 22-25], there are different types of instruments to do a survey: self-administered questionnaires, interviews, structured record reviews or structured observations. In this thesis I will use self-administered questionnaires in which participants answer the questions and complete the questionnaire by themselves.
According to J. Lazar, J. H. Feng and H. Hochheiser [LFH10, p. 116], the questions can be in

printed form or online. My survey will be an online survey with closed-ended questions as they are described in [LFH10, p. 112] and [Fin03b, pp. 36-38]. For this online survey the questions have to be well-formalized. It is important how questions are asked to get correct information. That is why I formulate my questions the way J. Lazar, J. H. Feng and H. Hochheiser [LFH10, p. 113], H. Bernard [Ber00, pp. 241-246] and T. Punter et al. [PCFJ03] suggest to do. Detailed information about the survey will be explained in the chapter 'Survey'.

After developing the guidelines, I will reflect the self-developed open source mobile application project with my guidelines. I will focus on the following questions: 'Which guideline did I implement/use in my application?' and 'What was the reason for not using some guideline?'. Of course the experience of developing the mobile application will influence the creation of the previously mentioned guidelines.

1.4 State of the Art

Nowadays smartphones are used by more and more people. IDC announced in a recent press release [weba] that 722.4 million smartphones were shipped in 2012. In contrast to that, they reported in another press release [webc] that the personal computer shipment for the year 2011 was about 353.3 million PCs worldwide and that for the year 2012 it would just be 371.1 million. Reuters shows a similar result in their diagram [webd]: the sales figures of smartphones are higher than those of traditional personal computers.
A smartphone is a very personal device. You can call somebody, write short messages, take pictures, browse the Internet, write e-mails, look up what the weather will be like in the next days or connect to your social community. And you can do all these things wherever you want to - you are not restricted to your home or to your office. It is obvious that for many people a smartphone is a very important device nowadays.

Community platforms have become very popular within the last years. In March 2013 Facebook[3] - probably the most prominent example - had, according to their first Quarter 2013 Results [webb], 665 million daily active users. Google+[4], the social network by Google, had about 343 million active users in December 2012 [Pet].
Millions of users use social networks to communicate, share information or do other things. More and more people access their social network and do these things with their smartphone. For example, 100 million users of the social network Facebook accessed and used it with their mobile device in the year 2010 [Pal]. At that time Facebook had about 500 million active users [Joh]. So every fifth user used Facebook with a mobile device.
Mobile applications are very important. This becomes obvious when taking Facebook as an example. They developed not just one application to access the social network, but four: Face-

[3] http://www.facebook.com
[4] https://plus.google.com/

book[5], Facebook Messenger[6], Facebook Pages Manager [7] and Facebook Home[8]. All of them should help to access and use the social network: with Facebook (the application) the users can use Facebook from their mobile devices, with Facebook Messenger users can easily communicate with other users from Facebook, with Facebook Pages Manager users can administrate their Facebook pages and Facebook Home replaces the traditional home screen of a smartphone and makes Facebook the center element of their smartphones and tries to integrate the users even more in the social community.

Trust in social networks and in mobile applications is a very important topic. Without trust a community cannot work and applications would not be installed. Papers about how trust can be generated in community-based mobile applications will be presented in the chapter 'Related Work'.

1.5 Structure of the Work

The thesis consists of an 'Introduction' in which the paper is motivated, problems are described, and the state of the art is presented. It describes the aim of the work, the methodological approaches and the structure of this work.
Chapter 'Basic Terms' defines and explains the main terms of this thesis: trust, community, smartphones and mobile applications. Trust is a very complex term which I try to describe in all its facets.
In 'Open-Share-It' I introduce the mobile application which I developed along with this thesis. In this application, trust has a major role. Experiences and ideas from developing this application influence the creation of the guidelines of this thesis.
In the chapter 'Related Work', I present and describe papers which give useful pieces of advice that can be used for the guidelines. The suggestions from other areas like e-commerce are examined and adopted so that they can be used for the guidelines.
In 'Interviews' the participants, the type of interview and the interview's results about trust for community-based mobile applications are described. The interviews will help to find approaches for the guidelines.
The chapter 'Survey' is about the way the survey is carried out as well as about its results.
In 'Guidelines for Trustful Mobile Applications' I develop guidelines which should help developers to build more trustful community-based mobile applications. The results of my research, interviews and surveys are synthesized into guidelines.
In the next chapter 'Comparison to the Open-Share-It Project' I compare the guideline's results with my self-developed application. I describe which guidelines I used and why others were not used in the mobile application.
Finally, the chapter 'Conclusion and Future Work' summarizes the results and gives an outlook for the future.

[5] https://play.google.com/store/apps/details?id=com.facebook.katana&hl=de

[6] https://play.google.com/store/apps/details?id=com.facebook.orca&hl=de

[7] https://play.google.com/store/apps/details?id=com.facebook.pages.app

[8] https://play.google.com/store/apps/details?id=com.facebook.home

1.6 Additional Information

The Open-Share-It project should have cooperated with Foodsharing. Because of that, it will be mentioned in some chapters. Further information can be found on the website: `http://www.foodsharing.de`. For a better readability this reference will not be displayed every time. The same goes for the operating systems iOS by Apple and Android by Google: please visit `http://www.apple.com/ios/` for more information about iOS and `http://www.android.com/` for more information about Android. Facebook is another company which will be mentioned in this thesis: for more information please visit `https://www.facebook.com/`. Other companies and websites are directly referenced with footnotes.

In some chapters additional information can be found. These pieces of information are written in italics and in grey color. They are not necessary for the understanding of the thesis, but they refer to additional figures or explain how the guidelines have been developed.

1.7 Summary

In this introduction I described my thesis in more detail. I outlined the current situation and why trust plays an important role in community-based mobile applications.
One aim of my work is to show the importance of trust in software development. Only a few papers give advice on this specific topic. So one aim of this work is to find approaches and develop guidelines for more trustful community-based mobile applications.
To reach these goals I explained the methodological approach which I use in my thesis: literature research, an interview and a survey.
I described the 'state of the art' about community platforms and smartphones, presented how this paper is structured and gave a short description of what the reader can expect in these chapters.

CHAPTER 2

Basic Terms

Before presenting and discussing the results of the different approaches and describing the Open-Share-It project, the basic terms have to be explained and defined. The aim of this thesis is to develop guidelines to enrich mobile community-based applications with more trust. Therefore, I explain the terms ’trust’, ’community’ and ’smartphone’ in this chapter for a better understanding and a clear definition as they are the key elements of this thesis.

2.1 Trust

As already explained above, trust is very important in this thesis. Therefore, the term trust is examined in this section. For trust there exists no clear definition. Because of that, some definitions are presented in the part ’Definition of the Term ’Trust’’.
The roles of the trust-relationship and the different phases (also called stages) are described in ’Roles of Trust and Phases’.
There are different types of trust. Once again, there is no clear definition and one can look at them from different points of view. Two classifications of trust types are explained in detail in ’Types of Trust’.
Trust cannot only be defined by its roles, phases and types, but also by its characteristics that help to understand the term trust in a better way. I list them in ’Trust Characteristics’.
Last but not least, in the part ’Trust in Software Development’, I explain trust in the context of software development and discuss security and privacy in this context.

Definition of the Term ’Trust’

Trust plays an important role in our daily lives: in ’real life’ as well as on the Internet. We could not buy anything on the Internet without some sort of trust. Neither could we travel by plane. In nearly every decision we have to make day in and day out, trust plays an important role.
However, there are many different definitions of trust. It is a term that is used in many different areas. For example, trust is discussed in papers about formal logic (e.g. [BBK94]), in papers

about security (e.g. [Jøs96]) or electronic commerce (e.g. [BS02]). Nevertheless, there is no general definition of trust.

For example, C. Johnson-George and W. C. Swap argue that a trust characteristic is the '[...] willingness to take risks [...]' ([JGS82] cited in [MDS95, p. 712]).
T. Grandison and M. Sloman [GS00, p. 3] define trust as

> [...] the firm belief in the competence of an entity to act dependably, securely, and reliably within a specified context [...]

Z. Weiguo, L. Jun and W. Bingshan describe trust as the '[...] glue that holds a community together.' [WJB08, p. 2117].
Similar to T. Grandison and M. Sloman, the authors S. Tseng and B. J. Fogg [TF99, p. 41] define trust as the following:

> Trust indicates a positive belief about the perceived reliability of, dependability of, and confidence in a person, object, or process.

Taking all definitions into account, this definition is the most appropriate one for this thesis. Therefore, it will be used in this thesis. On the one hand it shows that the result of the interaction with some person, object or process is not fixed, and on the other hand the definition makes it clear that trust does not only exist between two humans, but also between a human and an object or a process.

Roles of Trust and Phases

After describing some definitions and agreeing on one definition for this thesis, the roles of trust and the different phases can be explained.
According to R. Song, L. Korba and G. Yee [SKY07, p. 5], there are two different kinds of roles:

- Trustor
- Trustee

The trustor is the subject that trusts the trustee [SKY07, p. 5]. In the following I will use these terms to differentiate these roles.

According to D. M. Rousseau et al. [RSBC98] this relation - trust - has three different development phases:

- Buidling
- Stability
- Dissolution

The ’building’ phase is the beginning of the trust relationship between trustor and trustee [RSBC98]. In the phase ’stability’, trust already exists and in ’dissolution’ the relationship between trustor and trustee ends [RSBC98]. The trustor does not trust the trustee anymore.
In [FAMA12] S.J. Fusco et al. differentiate between three different stages of trust:

- Creation
- Development
- Maintenance

The first one is similar to the phase ’building’ in [RSBC98]. While the stages mentioned above only focus on the trust building and maintaining, D. M. Rousseau et al. [RSBC98] take into account that trust can and will be broken after some time.

Types of Trust

Just as there is no clear definition of trust - there is no standard declaration of types of trust either. S.J. Fusco et al. [FAMA12] describe three forms of trust:

- Cognitive trust
- Emotional trust
- Behavioral trust

Cognitive trust is based on a ’good reason’ and does not need any further evidence [FAMA12, p. 41]. Emotional trust depends on the emotions between the trustor and trustee and is especially high in ’close interpersonal trust’ relationships [FAMA12, p. 41]. Behavioral trust is based on behaviors, like communication [AEG+10]. According to S. Adali et al. [AEG+10], the trust between trustor and trustee results in some behavior that can influence trust again.

According to [WJB08] and [ARH00], there is another classification of trust as well:

- Dispositional trust
- Interpersonal trust
- Institutional trust

Dispositional trust can be described as ’personality-based’ [WJB08, p. 2117] or as a sort of fundamental trust [ARH00]. According to [ARH00, p. 3], it is the trustor’s ’[...] general trusting attitude [...]’. Interpersonal trust is the trust between two agents [WJB08] [ARH00].
The last one - institutional trust - is also called impersonal trust [WJB08]. It does not rely on the trustee, but on ’perceived properties’ on the institution in which the user does his/her trusting action [WJB08, p. 2117] (for example: the community network in which the trustor and trustee communicate). A. Abdul-Rahman and S. Hailes [ARH00, p. 3] call it ’System Trust’ because it is the trust in the system and not the trust in another person, process, object etc.

Trust Characteristics

Trust between trustor and trustee is a complex relationship that depends on different factors. In their paper [ARH00] A. Abdul-Rahman and S. Hailes list some characteristics of trust:

- Uncertainty
- Dynamic
- Non-monotonic
- Non-transitiveness
- Decisions, based on trust, can differ from rules for rational choice theory

Uncertainty mentioned by [ARH00] means that when a trustor trusts in a trustee, the result of this trust is uncertain. Trust can change over time and can increase or decrease. Therefore, another characteristic of trust is that it is dynamic and non-monotonic [ARH00]. According to A. Abdul-Rahman and S. Hailes [ARH00], non-transitiveness is another characteristic of trust. When user A trusts in user B, and user B trusts in user C, we cannot assume that user A trusts in user C.
T. Grandison and M. Sloman [GS00] explain that in some scenarios trust can be transitive. I am of the same opinion that trust has not to be transitive in general, but there are some cases when users indeed will trust other users according to transitiveness (for example in signatures for public keys in 'web of trust' or perhaps in a friendship-system).
The last characteristic feature described in [ARH00] is that the decisions, based on trust, can differ from the rules as we know them from rational choice theory ([Bar83] and [Gam90] cited in [ARH00, p. 3]). Trust is complex and simple rules cannot apply to all possibilities (in my opinion).

In [GS00] they explain that trust depends on the context. For example: A user may trust another user in a social network more or less than if they would meet in real life, or the user trusts another user because of his role in the company. Therefore, trust does not only depend on the trustee, but also on the context.

Of course these characteristics are not a complete collection of all the characteristics of trust, but those mentioned already give an impression of how complex trust is.

Trust in Software Development

Trust is a very important topic in software development. If users cannot trust other members or the software, the users will feel uncomfortable or will just not use it. Especially because of the development of social communities trust is an important topic. Members interact with each other and share information and therefore, they have to trust the other users.

When people think about trust, they often think that it is a consequence of security [Uli05].

People believe that a secure environment can create trust [Uli05]. This assumption is incorrect according to F. Ulivieri [Uli05] because security does not implicate trust. According to F. Ulivieri [Uli05], every secure environment will be insecure some day, because technology is getting better and better. In [Uli05], the fact that an environment is secure and can never be hacked is called the first illusion. The second illusion, explained by F. Ulivieri [Uli05], is that such a secure environment gives the users the feeling of trust. They would feel secure in such an environment, but they would not have the feeling of trust [Uli05] [Nis99]. In my opinion, even the opposite can happen: a system that is very secure, can lead to less trust.
However, security is important to generate trust. F. Ulivieri [Uli05] mentions that not only 'real security' is important, but also 'perceived security': the security that is recognized by the user. Otherwise, when users do not believe in the security of the environment, security itself makes no sense [Uli05].

Z. M. Aljazzaf, M. Perry and M. A. M. Capretz [APC10] point out that both security and privacy are important to create trust.
Therefore, privacy is another important issue that is linked with trust. D. Moreland et al. [MNHZ10] explain that security mechanisms alone are insufficient because they can be broken and privacy issues have to be considered.
Trust is positively correlated to privacy [Kos10]. People may share private information with others because they trust them. But privacy is negatively correlated to trust [Kos10]. This means that if the user is concerned about his privacy and does not share some of it with others, for example his identity, others may trust this person less.
According to D. Moreland et al. [MNHZ10], trust can amplify security and privacy of a system. Apart from other facts, we can say that trust is influenced by security and privacy. Trust is not completely generated through security and privacy, but it has an important role and should be given special attention in software development where trust-building is important.

2.2 Online Communities

Trust is often relevant in communities and is one focus of this thesis. Therefore, I describe and define it in 'Definition of the Term 'Online Community''. The difference between online and offline communities is discussed in 'Assumption for the Thesis'. I also set an assumption regarding community members for this thesis.

Definition of the Term 'Online Community'

Communities or social networks are not new inventions: Mankind has always worked together in groups to generate things that would not be possible without the help of others [SLD11]. However, the term has changed over time.
With the 'Web 2.0' social communities like Facebook or StudieVZ [1] have become popular. According to G. Zhang and E. K. Jacob [ZJ12], we have to distinguish between offline and online communities. A general definition of community is [Rei97, p. 43]:

> A "community" is group of people sharing a common interest and set of values.

G. Zhang and E. K. Jacob [ZJ12] explain that with the introduction of social networks the term community has changed. Whereas traditional communities are geographically bounded, members of an online community do not have this restriction [ZJ12]. R. N. Yale [Yal11] explains that online communities can be of different kind. According to him, groups on the Internet can be more or less like a real community and it depends on the count of gratifications which are fulfilled in it [Yal11].
In my opinion, it is often difficult to estimate how 'real' a community is. On Facebook, for example, users have friends that they know from real life, but on the other hand, users also add other users as friends who they do not know in real life.

Assumption for the Thesis

Users may know each other before being in an online community or interacting with the other user. Especially for the feeling of trust this difference is important: a user who knows the other person and shares a common history with this person, may trust this person in another way than an unknown person. In this case trust can already be established. However, even in this case, trust in the context - the social network, the mobile platform, etc. - has to be created.
To make things easier, I will only distinguish between online and offline communities (and not any mixed form). For the rest of this thesis I assume that the users do not know each other, but want to interact with each other. With this assumption the guidelines can focus on how trust can be generated with a mobile application between two unknown parties (and how trust can be generated between the application and the user).

[1] `http://www.studivz.net/Default`

2.3 Smartphones and Mobile Applications

After defining trust and community, smartphones and mobile applications have to be investigated. First, I explain the main functions of a smartphone and the different existing operating systems and define on which operating systems this thesis will focus.
More and more people use smartphones in their daily lives as I already explained in 'State of the Art'. They help people to be connected with their community and give the users of such community platform the feeling of being online all the time. This is the reason why community platforms on mobile devices are such an interesting topic. Trust is very important for a community platform in general, but also in the context of smartphones. People often do not use mobile applications because of some security, privacy or trust reason as I explain in more detail in 'Trust in the Context of Smartphones'.

Definition of the Term 'Smartphone'

Nowadays, smartphones are very common and replace the traditional cellphone. The components of a smartphone get cheaper, and as a consequence, more and more people can afford a smartphone.
A smartphone in general is a cellphone with an operating system where you can download and install applications to enrich functions [WLZS11] or user experience. In [BBRS06, p. 70] they explain that the smartphone is the first pervasive computer and call them 'ubiquitous input devices' because you take them with you anywhere and therefore, you can access them at any time. It can also be described as '[...] complicated devices like mini computers.' [LY09, p. 617].
In contrast to an ordinary computer, a smartphone often has different kinds of sensors, for example: GPS to locate your position, a light sensor to adjust brightness of your display, a camera at the front of the smartphone and at the back to take pictures, a touch screen for user input, etc. With these sensors and the wireless connection to the Internet, applications with different kinds of functions and experience can be developed.
L. Wang et al. [WLZS11] describe the main functions of a smartphone as:

- Common functions of a cellphone
- Connectivity to the Internet
- Functions of a PDA (personal digital assistant): multimedia application, webpage browsing, tasks and agenda scheduling, managing e-mails
- It has an operating system with the ability to install applications
- 'The feature of humanity, may expand the functions of the cellphone to satisfy individual need [...]' [WLZS11, p. 688]
- Expandability by using third-party software

Therefore, I claim that a smartphone can be seen as a hybrid between cellphone and computer. On the one hand it has all the functions of a cellphone, and on the other hand it has all the

characteristics of a computer.
Nowadays, the number of operating systems for smartphones increases. The most common operating systems are:

- iOS
- Android
- Windows Phone 7[2]

There are also other operating systems, but they are rarely used or still being developed. For example: Firefox OS[3], Ubuntu Phone [4] or Blackberry 10[5].

In this thesis I will especially focus on iOS and Android because they are the most used operating systems at the moment. IOS and Android are installed on 87,6% of the smartphones shipped in year 2012 [weba]. Although my guidelines will focus on iOS and Android, most of my suggestions - if not all - can be used in other operating systems as well.

Trust in the Context of Smartphones

A smartphone is a very personal device and is often used by only one person [BBJ11]. In contrast to that, other devices like the TV, the camera or the personal computer are used by more than one person [BBJ11]. Especially for target marketing this factor is very important [BBJ11]. Of course, owners of a smartphone may be concerned about its security because personal data such as photos, contacts and e-mails are stored on their smartphones.
E. Chin et al. [CFSW12] interviewed 60 people about security and privacy issues on mobile phones and laptops. E. Chin et al. asked users if they would enter their SSN, shopping information (like credit card number), health data, bank account data and other personal things. They explored that 62,5% of the smartphone users did not want to use an application because of security reasons. In comparison to that, the partipiciants were more concerned about privacy on their smartphones than on their laptop. Some of them argued that their smartphone stores more personal information (e.g. their location and phone numbers) than their laptop. E.Chin et al. [CFSW12] asked the participants about their primary concerns about their phone: The participants answered that they feared the loss and damage of their phone, data loss and had concerns about signal strength and battery life. But participants were also concerned about trusting in their applications [CFSW12].
As already explained in the section about trust: security and privacy influence trust. With this relation in mind it is easy to see how important the feeling of trust in the context of smartphones is. E. Chin et al. [CFSW12] showed that for many users privacy, security and trust are important factors for using mobile applications.

[2] http://www.windowsphone.com/en-gb
[3] http://www.mozilla.org/de/firefox/partners/
[4] http://www.ubuntu.com/phone
[5] http://us.blackberry.com/software/smartphones/blackberry-10-os.html

2.4 Summary

In this chapter I introduced three different terms: trust, community and smartphone. They are the basic terms for this thesis.

In the first section I defined trust. I argued that trust is a complex topic. It consists of different roles and phases and trust can be divided into different types. Trust has different kinds of influence factors and I described that security alone is not the solution to make a software more trustful in software development.

Communities, as explained in the second section, can be divided into offline and online communities. Online communities can even be more or less like an offline community. For this thesis I focus on online communities: the users do not know each other, but want to interact with each other.

The last section was about smartphones and mobile applications. Mobile applications are an important way for community platforms to reach their users. In this subchapter I described smartphones, their key features and the existing operating systems. This thesis focuses on the operating systems iOS and Android because they are the most common ones.
I explained that generating trust in mobile applications is very important. People do not use mobile applications because they think the mobile application or the network is not secure or do not want to store their private information on a smartphone.

CHAPTER 3

Open-Share-It

For the master thesis I develop a mobile application for the operating system iOS. As I will explain in this chapter, for this application trust is crucial. It is a good example for a community mobile application. In the chapter 'Comparison to the Open-Share-It Project' I will compare it to the resulting guidelines.

In the following I introduce the project and explain how it is related to this thesis. In 'Description of the Project' I introduce the project and its context. A detailed description can be found in 'Features and Functions'. In 'Features for Further Versions of the Project' I explain features which will be part of further versions but could not be included in the first version. In 'The Focus on Trust' I describe why this project is so important for this thesis and which influence trust has in this application.

Please note that the project is still under development. Its design, icons, structure, features, terms and other things might change. The project is described from the current state of development and of course it can change until the first version is published.

3.1 Description of the Project

In our daily lives it often happens that we buy food and dump it some days later because we cannot eat or do not need it anymore. So, although the food could still be eaten, we dump it.
At the Vienna University of Technology, at the Institute of Design and Assessment of Technology, an open source project has been developed under the leadership of Eva Ganglbauer which faces this problem. The Open-Share-It project has been created for the operating systems Android and iOS and has an open source license. Because of that, it is free to adopt and to use. The project uses 'extreme programming' as software development method and is currently being developed in a team of seven people.

The idea behind the project is to develop a platform where users can share their food with other users if they do not need or want the food anymore. With this idea less food should be wasted and dumped.
The platform shows so-called ’foodbaskets’ on a map or on a list nearby of the current location of the user. A ’foodbasket’ is a term for one or more food items that the user wants to give away. A user can create such a ’foodbasket’ if he/she wants to share some food. Other members can select it and can make an appointment to get the items of a ’foodbasket’.

At the beginning, our idea was to cooperate with Foodsharing because they had a similar idea and they already had the infrastructure and a web-platform. But because of problems of cooperation we decided to develop it as an open source project.
The ’Wiener Tafel’[1] was interested in the application, and therefore, we decided that we might adopt it to a special edition: in the application a foodbasket is now presented as a ’Sackerl’ (= the German word for bag). Because of that, the presentation of the application in the current version consists of bags. But apart from its name and its appearance there is no difference to the objects called foodbasket. Because of that, I call them foodbaskets in this thesis.
In the meantime Foodsharing expanded and adopted their platform for Austrian users[2]. Currently, we are in discussion with Foodsharing to adopt it to their platform again.

3.2 Features and Functions

In the following, I describe different features and functions in detail which are implemented or considered for the first version of the Open-Share-It application. Because of space considerations only the most important pictures are displayed in this chapter. Other pictures can be found in the ’Appendix’. A note is added to the description of the function if a picture is added in the ’Appendix’.

Search and Watch Foodbaskets on Map View

If the user opens the application for the first time, he/she will immediately see foodbaskets on a map of his/her area (see figure 3.1). For this feature the user does not have to be logged in. So the user quickly gets an impression of what is going on in this area and can test some functions and get familiar without being forced to register himself/herself.
To protect the members of the community, the user who is still not logged in and therefore anonymous - can zoom in on the map only to a certain point, so that he/she can not locate the exact position of the foodbaskets. After logging in (see feature ’Log in and out’) the user can see exactly where the foodbasket can be taken from and can watch details (see feature ’Watch a Foodbasket’) of the foodbasket and request it (see feature ’Request a Foodbasket’). In the search bar the user can search for other locations and watch the foodbasket in this area on the map. With the location button in the right upper corner he/she can reset the postition of the map to his/her own current position.

[1] `http://www.wienertafel.at/`

[2] `http://at.myfoodsharing.org/`

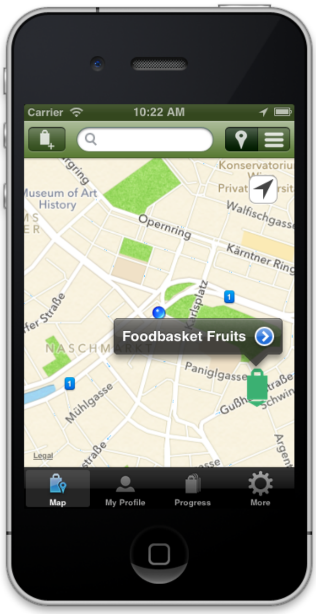


Figure 3.1: Map view for a not logged in user in the Open-Share-It application.

Search and Watch Foodbaskets on List View

Apart from watching and searching foodbaskets on the map, the user also has the ability to watch and search them in a list view (see figure 3.2). If the user switches to the list view the results of the map view will be displayed in a list. This list can be sorted by ’closeness’, ’actuality’ and ’collection time’. By default the list is sorted by ’closeness’: the closest foodbaskets will be presented first. With ’actuality’ the foodbaskets are sorted by the date when they were created and published to the system. The option ’collection time’ sorts the foodbaskets by their expiring dates.
Again, the user has the possibility to watch a foodbasket in detail (see feature ’Watch a Foodbasket’) and to request it (see feature ’Request a Foodbasket’) if he/she is logged in.

Register

The user can register for the community. Therefore, he/she has to enter his/her name, an e-mail address (twice) and a password (twice). Before the registration process is completed, the user has to accept the legal information and gets an e-mail afterwards to verify the e-mail address. After this process the user can log in with his/her e-mail address and password.

Note: a screenshot can be found in the Appendix: figure A.1

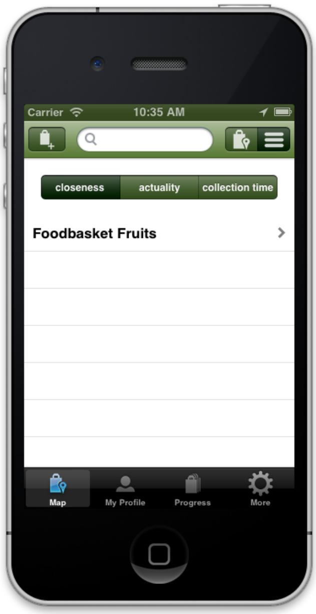


Figure 3.2: List view for a not logged in user in the Open-Share-It application.

Log in and out

To identify the user and to protect the others, the user has to identify himself/herself for some actions. Therefore, he/she has to enter his/her username and his/her password which he/she chose in the registration process (see feature ’Register’). Alternatively, the user can log in with his/her Facebook account (if the user added it to the account).
After logging in the user can do the following additional actions:

- ’Create a Foodbasket and Publish it’
- ’Request a Foodbasket’
- ’Answer a Request for a Foodbasket’
- ’Rate Foodbasket Owner’
- ’Rate Foodbasket Requestor’
- ’Edit Account and Private Information Settings’
- ’Manage Foodbaskets’

In addition, there is no restriction when zooming on the map.

Note: a screenshot can be found in the Appendix: figure A.2

Watch a Foodbasket

A foodbasket on the map can be watched in more detail. A foodbasket consists of different items (at least one), has a title, a description, a state, an expiration date and an address. The foodbasket will be displayed on the map according to the address that is assigned to the foodbasket.
An item of a foodbasket can be any kind of food that the user wants to share. For example, a foodbasket with the name 'Things from my fridge' could contain items like 'pizza' and 'chicken nuggets'. An item consists of name, weight, amount, purchase and expiration date. For every foodbasket and every item a picture can be added.

To make it easier for the reader to assume what a foodbasket contains, an ER-diagram of the structure of a foodbasket is shown in figure 3.3. Please consider that, for simplification reasons, this foodbasket diagram is not complete: e.g. there is no relationship to its owner or any requestor. This diagram should only give the reader a quick overview of the elements of a foodbasket.

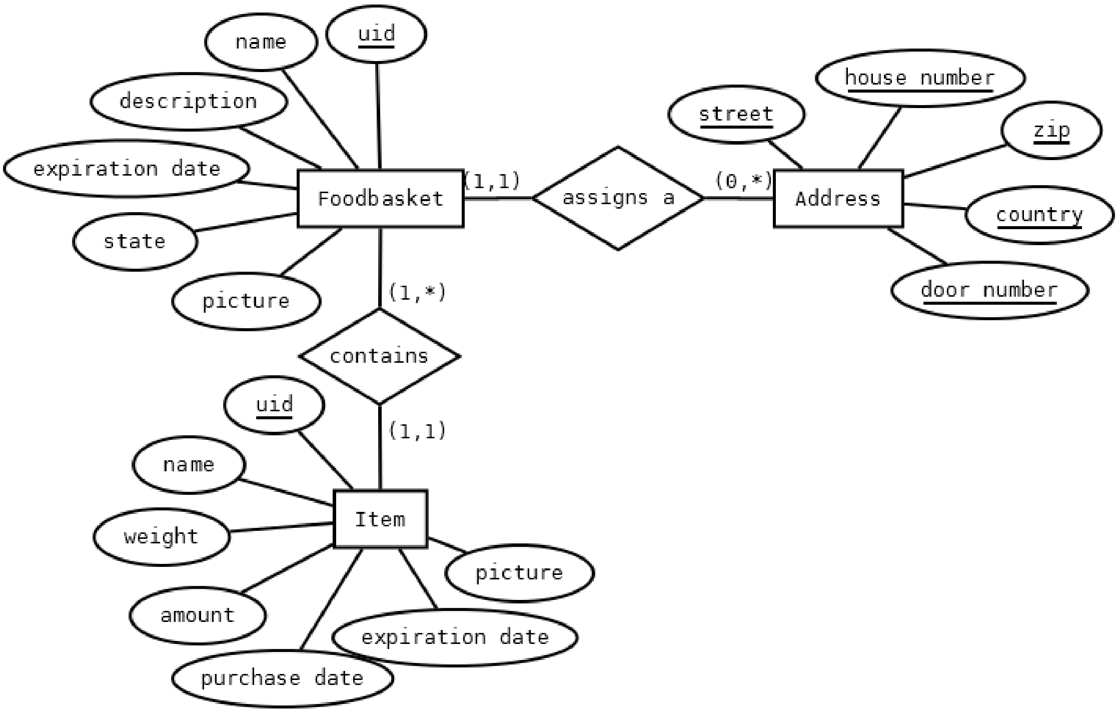


Figure 3.3: A simplificated ER-diagram of a foodbasket.

There are some restrictions because of privacy considerations. When the user wants to watch a foodbasket and is not logged in, he/she can only read the first name and the first letter of the second name. For example, my name would be displayed for an anonymous user as 'Thomas W.'. He/she cannot request a foodbasket (see feature 'Request a Foodbasket') and cannot see the address. The address of the foodbasket is only displayed to users who have already agreed with the owner to take his/her foodbasket.

Note: screenshots can be found in the Appendix: figure A.3 and A.4

Request a Foodbasket

After the logged in user has chosen a foodbasket on the map or from the list and has seen the details, he/she maybe decides that he/she wants this one. In this case, the user can send a request to the owner of a foodbasket. Of course, this function is only possible for logged in members.

Answer a Request for a Foodbasket

If a foodbasket is requested, the owner of the foodbasket gets a notification that somebody sent a request. In this case the owner can, if he/she wants, first communicate with the requestor and then make an appointment or clarify open questions. If the provider of the foodbasket decides to give the food to the requestor, he/she can accept the request and they can meet in real life.

Rate Foodbasket Owner

After forwarding the food, the requestor can rate the owner of the foodbasket. He/she can rate him/her on a scale of 0 to 5: 0 is the worst and 5 the best grade. The requestor can also add some comment, so that other users can get an idea why he/she gave this grade or he/she can add additional information. For example, the requestor can describe what the handover was like, if the provider of the foodbasket arrived on schedule or in which condition the food was.

Rate Foodbasket Requestor

A transaction is always between two people at least, and therefore, the owner of the basket can also rate the requestor who took the food. He/she can rate in the same way as the requestor. With this rating system other users can see for example if a user is reliable and arrived on schedule.

Create a Foodbasket and Publish it

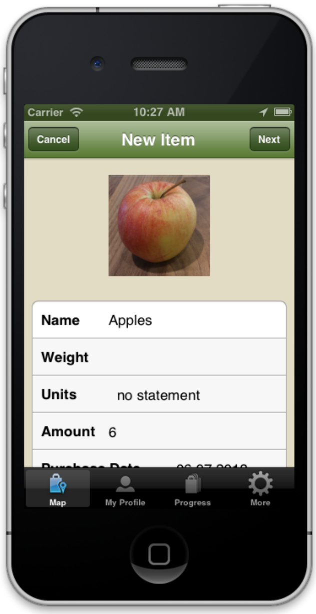
When the user is logged in he/she can create a new foodbasket by pressing the button in the left upper corner on the map or list view (see figures 3.1 and 3.2). First the user can create a new item. Information like name, weight, amount, purchase and expiration date (see figure 3.4 and the ER-diagram in figure 3.3) can be added. The user can add a picture by selecting one of his/her photo library or just take a new picture of the food. If no picture is chosen before switching to the next view, the user will be asked if he/she wants to add a picture.

After finishing one item, the user is asked if he/she wants to add another item or if he/she wants to go to the next view: the foodbasket view (see figure 3.5). If the user decides to go to the next step, the foodbasket view, different things can be done before publishing the foodbasket. First, the name of the foodbasket can be changed in the ’detail’ view. In this view an additional description can be added, a deadline to take the foodbasket can be defined and a picture can be added (optional) which should show the foodbasket.

The user can add other items in the foodbasket view, update items or delete items if it is desired. The address of the foodbasket is by default the address that is given for the account. The user can choose another address if he/she wants to. Therefore, an 'address manager' is implemented. The user can create, update and delete as many addresses as he/she wants to and assign one of them to the foodbasket (see figure 3.6). The addresses are linked with the account, so that for further foodbaskets the user can easily choose one which has already been added.

In the foodbasket view the user can see his/her account-information the way the others will see it. So the user can easily see what information will be displayed and can check them.

If the user has entered all the required information, he/she can publish the foodbasket by pressing the button 'Publish' in the upper right corner. After this action, the foodbasket is available for all members and can be changed or deleted in the progression view (see feature 'Manage Foodbaskets').



Name Apples

Weight

Units no statement

Amount 6

Figure 3.4: View for adding a new item to a foodbasket.

Manage Foodbaskets

The logged in user can watch, edit and create new foodbaskets in the progression view (see figure 3.7). In this view the user can manage his/her foodbasket and gets a summary of all the created foodbaskets. In this view all requested and taken foodbaskets can be seen. The user can easily check the state of each requested foodbasket.

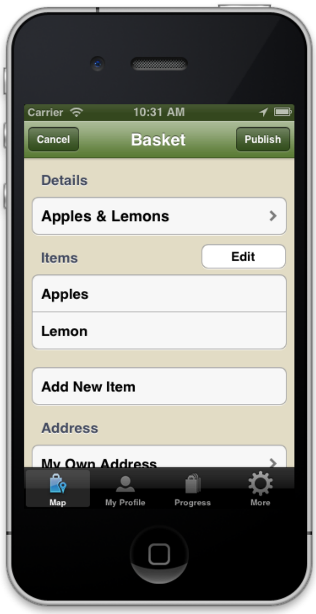
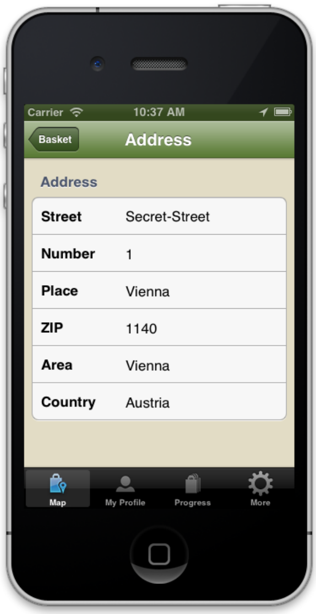


Figure 3.5: View for managing a new foodbasket.



Street	Secret-Street
Number	1
Place	Vienna
ZIP	1140
Area	Vienna
Country	Austria

Figure 3.6: View for creating a new address for a foodbasket.

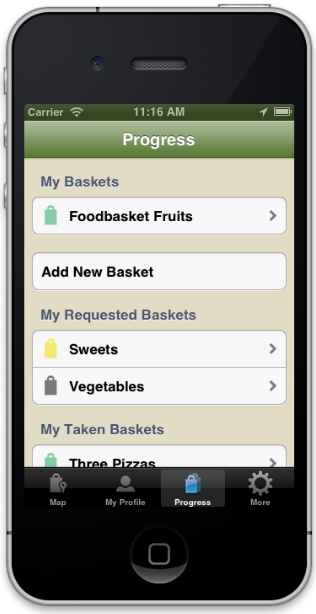


Figure 3.7: View for managing created, requested and taken foodbaskets.

Edit Account and Private Information Settings

Of course the user must have the ability to change his/her account information. The photo, name, mobile and phone number, e-mail address and password can be changed in the account views. The user can change the address that is linked with his/her account. This address will be used as default address for every newly created foodbasket.
He/she can see the ratings for his/her account and gets some statistics of how many foodbaskets he/she already gave away and took from others.

Note: a screenshot can be found in the Appendix: figure A.6, A.5 and A.7

3.3 Features for Further Versions of the Project

In our meetings we found other interesting features which would be nice if they could be added in further versions of the application. But because of lack of time we were not able to add these features in the first version.

Friendship or Following System

A friendship system in which a user is able to add other members of the network as friends would be an interesting concept for further versions. With this system the user would get informed if some of his/her friends added a new foodbasket and could assume the trustworthiness of the friends of a friend.

Another possibility would be a following system. In contrast to a friendship system, this relationship may only be found in one direction. The followed user does not have to confirm this relationship. The list of followed users may only be visible to the user himself/herself. With this system the user could get a notification if one of the followed users added a new foodbasket.

With both systems it would be possible to filter one's search or sort it according to one's friends or followed users. Both systems support an easier way to share food with one person more often because of a more focused view for foodbaskets.

Chat

At the moment the users of the social network have to communicate via mail or mobile phone. Therefore, it would be a good idea to make sure that the mobile application supports a secure communication channel. That way the users would not have to share any private information and would not have to switch to another application. With this solution it would be easier to communicate because all members would use the same channel. Other applications or some other hardware would not be needed in this case.

Searching for Food

The application already provides the possibility to search for addresses. These addresses can be of different quality. For example, if the user searches for the term 'Wien' he/she will be shown the city Vienna as a whole, but if he/she searches for the term 'Argentinierstraße 8, 1040 Wien', he/she will directly see the house at the place 'Argentinierstraße 8' on the screen. However, a search for food is not implemented yet. A category system would be another filtering option. For example, terms like 'fruit' or 'frozen food' would be another possibility to filter results and to precise the search result for the user.

Notifications

Notifications as already known from other applications like Facebook could be another feature for further versions. The user would get notified of new or changed foodbaskets in his/her area. For this function the user would not have to open the application to get these notifications. He/she would be informed by the notification center, and then he/she would be able to open the application if he/she was interested in this notification.

This would be especially attractive with the already mentioned friendship system. This would help to inform the users more precisely. If a friend added a new foodbasket in such a system, all his/her friends could be informed.

Another strategy for notifying users would be that the user can create favourites. These favourites could be the terms ’fruits’ or ’frozen food’ as already explained in the section ’Searching for Food’. With these favourites the user would be informed whenever a foodbasket is added that would match with the required term, for example: a foodbasket with fruits.

Report Abuse Button

In many areas, where users can create their own contents, a button to report abuse is implemented. With this button users can report about another content if they think that it should not be displayed in this area. For further versions this would be a good method that could be easily integrated to keep the network clean. Foodbaskets with odoriferous pictures or descriptions would be able to be detected. Foodbaskets that contain no content could be reported by users. Maybe even the users themselves could be reported.

This mechanism would be very powerful, but would have to be handled with care. In the background a strategy would have to be developed. Would reported foodbaskets be removed automatically? Would they temporarily not be visible after they would have been reported? Would they be checked by some member of the organisation? When would be intervened? What requirements would have to be fulfilled that a foodbasket or even a user would be removed or disabled?
These questions are not easy to answer and would have to be well-considered if implementing such a system.

Tutorial

Many applications have a tutorial when the user starts the application for the first time. The functions are explained with text, arrows or pictures and help the user to quickly understand the meaning of the application and how to use it. This would be a nice-to-have feature in further versions but it is only of minor importance, compared to other features.

Adaptation

Another feature which was discussed in our group was adaptation. Foodbaskets could be adapted, so that the user has a more personal experience and may identify with his/her foodbaskets. For example, foodbaskets could be displayed in different kinds of colors and patterns for users. With this modification other users could easily recognize foodbaskets from one person on the map. For example, a user could have red stripes on his/her foodbasket or an icon in front of it.

This feature would be elaborate and time-consuming. Other features have higher priority and need more attention, but it would give the platform a more individual feeling. However, we also did not consider this feature in our application because at the moment it is not considered on the Foodsharing platform.

3.4 The Focus on Trust

In many applications trust plays an important role, but especially for this application trust is extremely important. The user has to trust in many different areas. The user has to trust in:

- The mobile application in general (privacy, security, etc.)
- Other users when requesting a foodbasket
- Meeting other users in real life
- The food's quality that he/she receives

The user has to trust in the mobile application that his/her data are treated with respect and that his/her address and mobile number is not shown to users he/she does not want to. It is important that the user feels 'safe' in the environment and wants to share his/her information.

If the user requests a foodbasket, he/she has to trust in the user who offers the foodbasket. If he/she has no trust in the platform or in their users, the platform will not be used very often.

It is important that the users who share the food trust each other. Otherwise, they might not want to meet in real life. Therefore, the application has to try to create trust between the users. Of course, this trust does not only depend on the presentation and mechanisms of the application, but it can help to extend the feeling of trust.

When the users meet and the food is delivered, the requestor has to trust that the food is still eatable. To ensure this, in the legal information of the application it says that one is only allowed to share food that is still eatable: the expiration date must not be reached yet. However, the user still has to trust that these rules are obeyed.

Our team often discussed how these requirements could be realized. In this project trust is very important and has to be treated with a special focus.

3.5 Summary

Open-Share-It is a project developed at the Vienna University of Technology, at the Institute of Design and Assessment of Technology. With the help of the mobile application, users can share their food. Users, who would usually dump their food because they do not want to or cannot eat it, have the possibility to publish it on the platform. Other users can request it and make an appointment to get the food from the owner.

In 'Description of the Project' I explained the purpose of the application in general. I described how it was developed and which decisions were taken because of cooperating or not cooperating with organisations.

In 'Features and Functions' I listed all features that will be available in the first version of the mobile application. All the necessary requirements should be covered, like searching a foodbasket on the map, adding a foodbasket or requesting one. I described them and presented some current screenshots of the iOS application.

In the section 'Features for Further Versions of the Project' I gave an outlook on features that could be implemented in further versions. For example, a friendship system, as we know it from Facebook and other social networks, would improve the quality of search results for foodbaskets. A chat system, which can be used to make an appointment for the foodbasket, is also very important.

In the section 'The Focus on Trust', I explained why this application is so important for this thesis. Of course, the experiences of developing this application will affect the guidelines.

Trust plays an important role in many mobile applications. Open-Share-It is a good example for this. In this community-based mobile application trust is essential for the application's success, and therefore, should be handled with care.

CHAPTER 4

Related Work

The topic ’trust in community-based mobile applications’ is very specific and - as already mentioned - there are only few papers that describe this specific topic and give advice of how to improve trust in such applications.
But there has already been research in similar areas which can help to create the guidelines. There are many suggestions about trust in the area of e-commerce. The customer has to trust a webshop in many ways. He/she has to trust that his/her private data, such as name, address and credit-card number are handled with respect and are not used for other purposes. The customer has to trust that the delivered item is the same as the described one. If the customer pays beforehand, he/she has to trust that he/she receives the items afterwards.
Of course, only a little part of this wide spectrum can be presented in this chapter, but the papers to which I refer in my thesis will give some ideas from other areas that can be used and adopted for the guidelines that I present in the chapter ’Guidelines for Trustful Mobile Applications’.

4.1 Presentation Aspects

Design plays an important role in software development and can also enhance trust [Shn00] [SS03]. According to Ildemaro and Iván Araujo [AA03], the interface influences the trustworthiness of a website because it is the first thing a user sees. Ildemaro and Iván Araujo [AA03] explain that if the website is unstructured, not complete or even random content is provided, users might see the seller of a webshop as careless. Therefore, the navigation of the website should be well structured, the website should be easy to use as well as fast [AA03] [Koe03]. Browser-independence is another attribute mentioned by C. Hsu [Hsu08]. The content of the website should be well developed, so that the customer is not surprised when he/she receives the product [LH04].

According to C. Hsu [Hsu08], trust in e-commerce can be influenced by the factor familiarity. The user can trust more in a website if he/she understands the procedures of a website [Gef00].

For example, if a user already knows the procedure of purchasing an item - which information he/she has to share with the seller - this can give him/her a feeling of familiarity, and therefore, it may increase the trust in the website [Gef00].

P. Lanford and R. Hübscher [LH04] point out that it is important that the user has the feeling of control. For example, the user should be able to press the back button or decide when the order is completed [LH04]. Otherwise, I assume, the user might get the feeling of being ’controlled’ and restricted by the system.

4.2 Privacy Aspects

In the chapter ’Basic Terms’ I already pointed out that privacy and security play an important role for developing trust. In e-commerce privacy and security are also very important. Buying things can be very personal and the customer may not want to make private information or the things he/she buys public.
Ildemaro and Iván Araujo describe in [AA03] that the control of the own personal data is very important. According to them, the customer of a webshop should decide which data the seller obtains from him/her and should have the possibility to change them if he/she wants to. They also explain that the customer should decide if his/her data is accessible for third-parties. By default this should not be the case - the user really has to decide if he/she wants to give his/her data to third-parties [AA03].
Often, users have to face checkboxes in formulas for subscription of newsletters while they are buying things or registering on a website. These checkboxes should be unchecked by default. Otherwise, the user may think that he/she makes a wrong decision that is not allowed if he/she unchecks the checkbox [AA03] or he/she just does not see a possibility to uncheck it and later receives a lot of e-mails that he/she does not want [Koe03]. The user should have the feeling of control and not worry about making a wrong decision.

Moreover, a website (in the e-commerce area) should point out its efforts regarding privacy and security [AA03] [Shn00]. A website should have policies which are easy to find and read [Shn00], so that the user sees that the webshop owner is concerned about privacy and security. If the user reads these policies, he/she might trust the website more.

Even if such policies exist on a website, personal information should be cared with respect. Personal information about the users of a website should only be asked for, if needed [LH04]. For example, the credit-card number in a purchase process should only be asked at the end of an order when it is really needed [LH04].

The Federal Trade Commission published a report with the title ’Mobile Privacy Disclosures: Building Trust Through Transparency’ [Feda] in 2013. In this report they explain methods to make the use of the data and privacy decisions transparent. The user should figure out why the data is needed by the application to increase the user’s trust. Apart from the advice of using a privacy policy, they came to the result that mobile operating systems should support a notifica-

tion which informs the user when data is collected and gives him/her the choice to allow or not allow such a collection[1]. In the report [Feda] they show that in the iOS operating system this sort of mechanism is implemented for the use of GPS (see figure 4.1) [Feda].
The user in iOS has to allow the access of his/her own location, so that the application can use it.

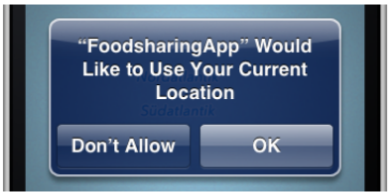

"FoodsharingApp" Would Like to Use Your Current Location

Figure 4.1: In iOS the user is asked if he/she allows the access to the GPS service by the application.

Another interesting result of the workshop carried out by the Federal Trade Commission [Feda] is the use of icons in operating systems. In iOS, for example, the user always knows when the GPS is used in applications because of an icon in the status bar (see figure 4.2). In my opinion, other consequently used icons (provided by the operating system) could increase trust because it makes actions transparent.

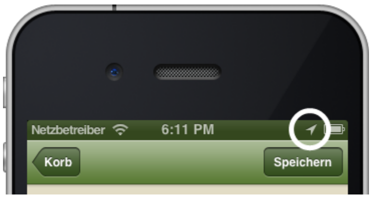


Figure 4.2: GPS icon in iOS: In iOS the user is informed when GPS is used by an icon in the status bar.

[1] also explained in [Fedb]

4.3 Technical Aspects

Presentation and privacy aspects alone will not be sufficient to create trust in a website. Promises from privacy and security policies such as transmitting data securely and on storing them securely have to be realized with the help of technology.

From a technical point of view different factors have to be considered which have an influence on trust. Ildemaro and Iván Araujo find the following areas that influence trust in e-commerce [AA03]:

- Security
  - Privacy and Confidentiality
  - Availability
  - Integrity
  - Authentication
  - Accountability/Non-repudiation
- Performance
- Scalability
- Compatibility

Ildemaro and Iván Araujo [AA03] list security as one important technological aspect to increase trust in an e-commerce platform. K. Siau and Z. Shen describe that security plays an important role in building trust as well [SS03]. They argue that, especially for mobile commerce where data is transmitted over wireless networks, security mechanisms like encryption and digital signatures are important and, as a result, can increase trust in mobile commerce [SS03].
According to Ildemaro and Iván Araujo [AA03], private information which the customer shares with the website should be treated confidentially and be kept private. The transactions between the customer and the webshop and the permanent storing of data should be encrypted, so that they are secure [AA03].
Availability is also mentioned by [AA03] in their security concerns. A system should have a high availability. This means that the system behind the webshop is running and available most of the times (in the best case it is always available). The availability can be increased by hardware and software solutions [AA03].
Another important feature in the security of an e-commerce platform is its integrity [AA03]. No unauthorized entity should be able to modify data [Sta07, p. 703]. Especially in e-commerce, in which money is transferred and orders are done, this attribute is important.
A feature listed by Ildemaro and Iván Araujo [AA03] is the authentication. The participants of a business transaction should authenticate them so that the identity of each other is known [Fer98]. Certificates are a way to authenticate an entity [Fer98].

The last feature listed in the security concerns by Ildemaro and Iván Araujo [AA03] is accountability and non-repudiation of the users. Others might behave better if there is accountability but it can violate anonymity and privacy [FKH00].

Performance is another technological key element in the list by Ildemaro and Iván Araujo [AA03]. Values for performance are the time that is needed to load the website, the download or upload time, the time needed to access the database, the processing time etc. [AA03]. For a good experience and to make the user satisfied, these values should be as minimal as possible.

For webshops which are accessed by many users it is important that they support scalability. If many users access a webshop in a short time, the response time can increase or even failures can happen [AA03]. Therefore, it is important, that for such cases, the platform can add hardware resources so that the increased access request can be handled [AA03]. These hardware resources can be released if the amount of users accessing the platform decreases.

The last aspect that Ildemaro and Iván Araujo list as technologically relevant to increase trust is compatibility. When developing an e-commerce platform the different browsers and plug-ins have to be considered [AA03]. This should be tested well, so that the user has a good experience and can establish trust when using the platform [AA03].

P. Lanford and R. Hübscher support their guideline 'Trust and Usability' with the advice to 'Show technical competence' [LH04, p. 318]. According to them, a website should be developed well so that no broken links on the website exist or pictures fail to load. Otherwise, (I assume) the user might doubt in the competence of the webshop provider and this may destroy trust.

C. Hsu writes in his paper about online trust [Hsu08] that perceived security and perceived privacy, as already mentioned in 'Trust in Software Development', can increase trust in the website.

4.4 Reputation Aspects

Apart from presentation, privacy and technical considerations, an e-commerce platform provider should consider reputation as well. Reputation is important for a website to earn trust and can be developed through different methods. Different kinds of ratings can influence the reputation of a website.

Rating systems as we know from many websites, like Amazon[2], eBay[3] or Stackoverflow[4] can enhance trust for the user [Koe03] [SY00] [Shn00]. According to S. Steinbrecher [Ste04], the

[2] http://www.amazon.com

[3] http://www.ebay.com

[4] http://www.stackoverflow.com

ratings give the seller a reputation so that the user can assume the future behavior of the rated seller. For example, if a seller has a very good reputation, this means that the customers rated the seller as very good and the user might assume that the seller will act in a correct way. But rating systems are not only useful to rate sellers: services, documents and other items can also be rated to enhance trust in them.

A company can enhance trust by providing information about past performances [Shn00]. Airlines for example present on-time percentages for flights [Shn00]. The website of Austrian's railway company ÖBB[5] for example explains that 96,5% of all the trains were on time in the year 2012.

A history of acting well can help to create trust for a company, even if they try something new [Koe03]. Lands' End, as described in [Koe03], was able to establish its webshop easily because customers had already a history with the company where customers were treated well.

Statements from previous users on the website can help the user to estimate the expected behavior of the website [AA03]. For example, Parship [6] provides 'success stories' from users who found their love on this dating platform. Couchsurfing [7] presents stories and images from members who travelled around the world.

Another possibility to establish trust is to use certificates from third-parties [Shn00] [SY00] [Koe03]. On websites logos from third-parties can increase the user's trust [Shn00]. Examples are: TRUSTe[8], Trusted Shops[9] or BBBOnLine[10] [SY00] [AA03] [Shn00] [Koe03]. The same is true for awards: displaying them on the website can increase trust [AA03].

Of course in the area of e-commerce the brand itself is very important. According to Yousafzai et al. [YPF$^+$05], brands represent quality and assurance. Therefore, it is important to establish a reputation: an e-commerce platform can advertise in different kinds of media to make its shop and name public [LH04].

[5] `http://www.oebb.at/de/Services/Puenktlichkeitsstatistik/`

[6] `http://www.parship.at/erfolgsgeschichten/index.htm`

[7] `https://www.couchsurfing.org/n/stories`

[8] `http://www.truste.com/`

[9] `http://www.trustedshops.com/`

[10] `http://www.bbb.org/us/bbb-online-business/`

4.5 Summary

Developing trust can be achieved in several ways. Trust is needed in different kinds of areas every day. There have been a lot of scientific investigations in this field, especially in the area of e-commerce. In webshops trust is very important because the number of visitors and the profit can depend on it.

In 'Presentation Aspects' I presented some advice of how trust can be increased in the presentation of a website. For example, the content of a webshop should be well presented and the navigation should be easy. The feeling of 'familiarity' and 'control' can help to create trust in a webshop.

In the section 'Privacy Aspects' I pointed out that the website should have a privacy policy and should be very careful with the user's data. The user should be able to control his/her data and should not be asked for any information which is not necessary. In addition, the Federal Trade Commission [Feda] presents solutions to increase trust through transparency in mobile applications.

In 'Technical Aspects' I showed different technical aspects that are important to enhance trust. Especially Ildemaro and Iván Araujo [AA03] describe many technical aspects. They explain, for example, that security, the performance of the system, the scalability and the compability should be considered. Other terms mentioned in this technical context are: to 'show technical competence' and the idea of perceived security and privacy.

Finally, in 'Reputation Aspects' I explained mechanisms to build a reputation. Rating systems are a possibility to enhance trust because the user gets an idea of the rated item. Another possibility to enhance the reputation of a website is to show performance of the past or to provide statements from previous users. A history of acting well can help to establish new areas and to win the trust of the consumers. Certificates from third-parties are another possibility to show the user that the webshop is trustworthy.
The last consideration about reputation is the brand itself. It can help to create trust in a platform, and because of that, establishing and creating a good brand might help to increase the user's trust.

CHAPTER 5

Interviews

In addition to literature research, which helped me to find aspects for creating trust in mobile community applications, I did interviews with people from the academic area. In the section 'Information about the Interviews' I explain a little bit more about the participants and how the interviews were held.
The most important results of the interview are presented in 'Results of the Interviews'. The results of the interviews will be used for the next chapters to create the survey and finally the guideline.

5.1 Information about the Interviews

The interviews were processed according to [GH02, p. 83]: first preliminary considerations were done, then the interview itself took place and at last the data were analyzed and summarized.

In the preliminary phase, I constructed questions that would be used as a guide through the interviews. But the interview was not restricted to these questions. I also asked additional questions in the progression of the interview[1]. Before starting the interviews a test interview was held to test the questions and to estimate the duration of the interviews.

In the second phase I held the interviews with 10 experts from different areas. All of them have some relation to the Vienna University of Technology: some of them study at the university, others studied there some time ago and others again work at the Vienna University of Technology. Two experts are involved in the Open-Share-It project. The interviews were, with the agreement of the interviewees, digitally recorded and are treated anonymously. Therefore, I call them experts A-J.

[1] [LFH10]: also called 'unstructured interview strategy' see p. 189

After having interviewed all experts, I analyzed the interviews. A summary is given in the section 'Results of the Interviews'. In the section 'Summary' an overall summary of the interview is presented.

5.2 Results of the Interviews

When talking with the experts and introducing the topic 'trust', most of the experts pointed out that trust is a complex topic. For example, expert A said:

> [...] Trust is very [...] context dependent and it also depends very much on [...] how the user perceives the system and what the system should do from the user's point of view [...]
> *([...] Trust ist sehr [...] kontextabhängig und hängt auch sehr stark davon ab [...] wie der Benutzer dieses System wahrnimmt und was das System aus Usersicht tatsächlich bewerkstelligen soll.[...])*

Expert A also mentioned:

> Trust [...] is quite [...] a multifaceted and multi-dimensional term.
> *(Trust [...] ist ganz [...] facettenreich und [ein] multi-dimensionaler Begriff.)*

Expert C explained the importance of trust for our society in the following way:

> [...][It] seems to be obvious, that societies only work if people trust each other and cooperate. People who never cooperate, but are always totally suspicious, are just somehow extinct [...]
> *([...][Es] hat sich offensichtlich herausgestellt, dass Gesellschaften nur funktionieren, wenn Leute einander vertrauen und kooperieren. Die Leute die nie kooperieren sondern immer total misstrauisch sind, sind halt irgendwie ausgestorben [...])*

Expert F said, when talking about trust:

> [...] Everybody fights with the trust-problem in principle [...]
> *([...] Mit dem Trust-Problem kämpfen ja im Prinzip alle [...])*

Therefore, a simple ultimate solution to generate trust is quite unlikely. That is why I asked my interview partners how trust can be enhanced in software engineering and especially in mobile applications with social networks.

Ratings

One possibility which nearly all experts mentioned was a rating system. Expert J argued:

> The users can rate each other and can draw conclusions whether they want to trust another person or not.
> *(Die User können sich gegenseitig bewerten und daraus auch Schlüsse ziehen, ob sie der Person vertrauen wollen oder nicht.)*

Expert F, when being asked how to enhance trust between users with the help of the mobile application, answered in the following way:

> [...] that's simply with ratings.
> *([...] da ist einfach halt mit Ratings.)*

Expert E thought that ratings alone would not be enough:

> If I, as a user, am really interested in it, then a bar with some percentage will not be enough [...] but I might want to have the possibility to go deeper and read about it [...]
> *(Wenn ich mich wirklich als User dafür interessiere, dann reicht mir so ein Balken mit so und so viel Prozent nicht [...] sondern dann will ich vielleicht auch die Möglichkeit haben sozusagen tiefer zu gehen und nachzulesen [...])*

Expert B said in this context:

> [...] if I can actually read what he has written, I can get an idea of how trustworthy this statement is because of its style.
> *([...] wenn ich tatsächlich das lesen kann was der geschrieben hat, dann kann ich mir über die Art wie er das geschrieben hat schon ein Bild machen wie vertrauenswürdig diese Aussage ist.)*

But grades and a description are not the only factors for a well-working rating system. Expert F explained:

> You need a critical mass. If you have one or two ratings, it is simply more difficult than if you have 30 ratings.
> *([...] Du brauchst eine kritische Masse. Wenn du ein oder zwei Bewertungen hast, dann ist es einfach schwieriger als wenn du 30 Bewertungen hast.)*

He also pointed out:

> It has to be clear that it is from real users.
> *(Es muss halt klar sein das des von echten Usern ist.)*

An important fact for generating trust in social networks is that the other user is a real user and not a fake user - a user who poses as another or even a system that pretends to be a user. Expert C said:

> What changes, so to speak, in social networks is that some intuitions that we had in personal in the past, are transferred [and] that this maybe does not always work well. [...] There are always people who can cheat very well in such personal interactions. Those are the typical confidence tricksters [...] Perhaps this is easier in the electronical environment.
> *(Was sich sozusagen ändert durch die sozialen Netzwerke ist, ist das manche Intuitionen, die man früher im Persönlichen hatte, übertragen werden [und] das vielleicht nicht immer gut funktioniert. [...] Es gibt ja immer Leute, die bei solchen*

> *persönlichen Interaktionen extrem gut betrügen können. Das sind diese typischen Trickbetrüger [...] Das ist vielleicht im elektronischen Umfeld leichter.)*

There are some possibilities to make it more difficult to fake other users. Ratings are one possibility, but there are also others.

Information

Another possibility to enhance trust in such networks and to make it harder to fool other users is to present more information about the user. Expert C explained:

> The more I know about a person, the more [...] I trust him.
> *(Je mehr ich über eine Person weiß, desto eher [...] vertraue ich dem.)*

Most of the experts agreed that information about users can increase the trust-relationship between them. Expert H explained this with an example of the career network Xing[2]:

> If there is a curriculum vitae that is mostly complete, then I can [...] rather imagine the person behind the profile [...]
> *(Wenn ein Lebenslauf da steht der eben halbwegs lückenlos ist, dann kann ich mir [...] unter der echten Person hinter dem Profil eher was vorstellen [...])*

Expert A took the Open-Share-It project as an example:

> With Foodsharing it could be interesting to stress the similarities.
> *(Bei Foodsharing könnts deswegen auch ganz interessant sein raus zu streichen was Gemeinsamkeiten sind.)*

Expert G argued:

> One rather trusts a profile, if there is a name, address and a photo given, than one that has only a nick-name.
> *(Man vertraut einem Profil eher wenn man einen Namen, eine Adresse und ein Foto dazu hat als wie wenn man nur ein Nick-Namen hat.)*

According to him and other interviewed experts, real-names can increase trust in social networks. But not all experts were of the same opinion. For example, Expert H said:

> I do not know him anyway [...] He can choose some name that also sounds like a real name.
> *(Ich kenn den sowieso ned [...] Er könnt ja irgendein anderen Namen angeben, der a nach ein echten Namen klingt.)*

While expert D said something similar, expert E mentioned the loss of reputation in an anonymous system:

[2] `http://www.xing.com/`

> If somebody is anonymous, then [...] [he] has no [...] incentive [...] to protect his name, because he cannot destroy his reputatation [...]
> *(Wenn jemand anonym ist dann [...] gibts eigentlich keinerlei [...] Anreiz [...] [den] Namen oder die Identität zu schützen, indem man seine Reputation [...] nicht verspielt [...])*

Expert A said:

> I would establish a hypothesis right away that you trust people with real-names much more [...]
> *(Also I würd sofort die Hypothese aufstellen, dass man Leute mit Real-Namen gleich einmal wahrscheinlich sogar deutlich mehr vertraut[...])*

But sharing information about users is a sensitive topic. Expert J described the balancing act of sharing information:

> If I disclose my name, then I have the guarantee that the other person trusts me more because he already knows something about me [...] on the other hand I also disclose my name to the app, that means I have [...] to get ensured that [...] my app does not use my name improperly.
> *(Wenn ich meinen Namen preisgebe, dann habe ich natürlich die Garantie, dass mir der andere mehr vertraut, weil er schon einmal was über mich weiß [...] andererseits gebe ich meinen Namen auch der App preis, das heißt ich muss [...] garantiert bekommen, dass [...] meine Appp meinen Namen nicht missbräuchlich verwendet.)*

Friendship or Following Systems

Expert J was of the opinion that other mechanisms are more important than showing more information about a user:

> I think that it is more important to have a following system [than additional information about the user]. I trust more in a user if a user is followed by some people or if I can see that the person is very active and has already been in contact with many other users.
> *(Ich glaube was wichtiger wär [als zusätzliche Informationen über den User], wär einfach, wenn man zum Beispiel so ein Following System hätte. Dass einem User bestimmte Leute follown oder [...] wenn ich sehe, dass diese Person sehr aktiv ist und mit vielen anderen Leuten in Kontakt getreten ist und die dem eben vertrauen, dann würde ich dem auch eher vertrauen.)*

Expert A explained a similar mechanism:

> [...] what they [social medias] also do, is that they strongly use the mediated trust model. [...] Members, who I find trustworthy, like something and it influences others this way. For sure there are chains of trust [...]
> *([...] was die [Social Medias] aber auch zusätzlich noch machen, ist, dass sie ganz*

> *stark auch diesen mediated trust model machen. [...] Leute in diesem Netzwerk, die man vielleicht vertrauenswürdig findet, die finden des wieder gut und so überträgt sich das. Da hat man sicher so Ketten von Trust [...])*

Privacy

Most of the experts agreed that privacy is a factor that can increase trust. Expert J told me:

> [...] My privacy is sacred to me!
> *([...] Mir ist mein Danteschutz heilig!)*

Expert A pointed out that information on smartphones is a very sensitive topic:

> It is another category of data that you can take [...]
> *(Es ist eine ganz andere Kategorie von Daten, die man da nehmen kann [...])*

Expert J said:

> [...] If the app simply knows where I am, what I am doing and where I am going - that leaves a bad taste [...]
> *([...] Wenn die App einfach weiß, wo ich gerade bin und was ich so mache und wo ich hingehe - das hat halt immer so ein Nachgeschmack [...])*

Therefore, privacy plays an important role to increase trust in mobile applications. Many experts claimed to make privacy aims more visible. Expert E discussed transparency as follows:

> Transparency as [...] a trustworthy measure [...] can be very important in many areas.
> *(Transparenz als [...] vertrauensfördernde Maßnahme [...] kann in vielen Bereichen [...] sehr wichtig sein.)*

Expert J said:

> [...] It should be clear [...] where one gives away some data and who can see them.
> *([...] Man [müsste] klar machen [...] wo man jetzt genau welche Daten hergibt und wer die auch sehen kann.)*

Expert B mentioned technical documents which should help to generate trust:

> I would try [...] to publish technical documents that somehow show 'okay, your data stays there and another user does not even have the possibility to hack into it
> *(Dann würde ich eigentlich versuchen[...] technische Dokumente [...] zu veröffentlichen, dass man irgendwie zeigt 'okay, deine Daten bleiben genau dort und ein anderer hat gar keine Möglichkeit sich dazwischen zu hängen [...])*

Security

Apart from privacy aspects, it is important that one's private information is securely treated. Therefore, security is another important topic. Every expert mentioned the importance of security in developing mobile applications. Expert C explained his work in the interview in the following way:

> [...] What we deal with are security-technologies and organizational security as a medium to reach trust.
> *([...] Womit wir uns beschäftigen sind Sicherheitstechnologien und auch organisatorische Sicherheit als ein Mittel Vertrauen zu erreichen.)*

Expert J said about security:

> I think that this is a basis for trusting in the whole thing. Because if that does not work, [...] then you can forget it.
> *(Also ich finde, dass ist so die Grundbasis dafür, dass ich überhaupt vertrauen habe in das Ganze. Weil wenn das schon nicht stimmt, [...] dann kannst es gleich vergessen.)*

Expert I stated:

> It is difficult: how can you see security as a user?
> *(Es ist problematisch: wie sieht man Security als User?)*

Mobile applications do not have standard symbols for encrypting data or something else at this moment in time. Expert J had an answer to this question:

> [...] because of that I believe that it is important that the user is told, 'We encrypt your connection [...]
> *([...] deswegen ist es glaube ich wichtig, dass man dazu sagt 'Wir verschlüsseln ihre Verbindung [...])*

But this requires trust again as expert I explained:

> You actually trust completely in the provider of an app.
> *(Du vertraust eigentlich komplett dem Anbieter der App.)*

Expert A explained that 'perceived trust' would be very important in this case because, at this moment in time, users in mobile application could hardly recognize security or could not find it at all:

> [...] Of course it is also important on a more interaction-interface level: how can one give the user the impression that the system is trustworthy [...]?
> *([...] auf einer mehr Interaktions-Interface Ebene ist es natürlich auch wichtig: wie kann man dem Benutzer auch tatsächlich vermitteln das dieses System vertrauenswürdig ist [...]?)*

Open Source

I asked the experts if open source projects have an influence on trust. Many experts think that a project that is developed as an open source project can increase trust. Expert F stated:

> Simply the fact that there is a possibility [to read the code] is very important. Because of that, open source is trustworthy for me.
> *(Alleine die Tatsache, dass die Möglichkeit gegeben ist [den Code einzusehen], ist schon wichtig. Sofern ist open source für mich schon trustworthy.)*

Expert G saw this in the same way:

> In open source the source code is accessible to everybody and because of that I am of the opinion that security holes can be found earlier and that again is a factor that increases trust.
> *(Bei Open-Source ist der Source Code für alle zugänglich und deshalb werden meiner Meinung nach Sicherheitslücken früher gefunden und das ist wieder ein Faktor der das Vertrauen in die Software erhöht.)*

Expert B explained this with the example of Android from Google:

> Maybe I do not trust Google, but I trust in the fact that [...] Google cannot risk to implement something [...] in [...] Android that is a privacy concern [...] because too many people could read that [...]
> *(Ich vertraue vielleicht nicht Google selbst, aber ich vertraue darauf, dass [...] es Google sich nicht leisten kann [...] in [...] Android selbst was einzubauen, was in irgendeiner Form Privacy Concern hat, weil [...] das können zu viele Leute anschauen[...])*

But open source also has some weak spots as expert C discussed:

> [...] that's why one finds weak spots easier in source code than in binary [...] I do not have to report the weak points [...] and that's why I might use them [...]
> *([...] dafür [...] findet man Schwachstellen auch halt viel leichter im Source Code als im Binary [...] Ich muss die Schwachstellen ja nicht melden [...] und dann kann ich es auch ausnutzen [...])*

Expert B explained that many people do not know the term open source and said:

> [...] First of all people have to understand what this means [...]
> *([...] es müssen die Leute überhaupt mal verstehen was das bedeutet [...])*

Therefore, even if open source can increase trust, the majority has to understand the meaning of such projects first.

Advertisement

When I interviewed the experts about advertisements in mobile applications, the opinions were divided. Some did not see any impact on trust whereas others did. Expert H did not see any correlation and said:

> A necessary evil [...]
> *(Ein notwendiges Übel [...])*

Expert E answered:

> I think many are already used to it by now [...]
> *(Ich glaube mittlerweile sind viele daran schon gewöhnt [...])*

Expert J is of another opinion than expert H:

> [...] I think that the [...] operators of the apps simply pursue another purpose with their app - to make money.
> *([...] Ich denke mir einfach, dass die [...] Betreiber der App, die da dahinter sind einfach einmal ein ganz anderen Zweck verfolgen mit ihrer Appp - nämlich die Geldmacherei.)*

Expert B made a similar remark concerning websites:

> If [...] a site contains many advertisements [...] then it generally decreases my trust into it very fast, because I think: that is a [...] money-oriented thing [...] they do not really care about usability and so on.
> *(Wenn [...] auf der Seite extrem viel Werbung [...] ist dann senkt das mein Vertrauen schon mal generell sehr stark, weil man sieht dann gleich: das ist eine [...] gewinnorientierte Sache, die [...] nicht sehr stark auf Usability und so weiter Wert legt.)*

Communication

According to expert E, communication is an element to increase trust:

> When it is about building trust: it often works through communication. [...] People [are] incredible good at finding out [...]. From short answers [...] one can get a more concrete impression than from some scale-ranking.
> *(Wenn es um die Vertrauensbildung an sich geht: so was funktioniert oft über die Kommunikation. [...] Menschen [sind] erstaunlich fähig viel abzulesen [...]. Aus kurzen Antworten [...] bekommt man einen sehr viel konkreteren Eindruck als irgendeine Skalabewertung.)*

Expert G also mentioned this element:

> In my opinion trust could be increased if I could communicate with the person.
> *(Aber es würde durchaus das Vertrauen steigern, meiner Meinung nach, wenn man mit der Person kommunizieren kann.)*

Expert J took the Open-Share-It project, in which we are both involved, as an example:

> I believe that it is good that we have the possibility in our [...] app to communicate over secure channels.
> *(Ich glaube einfach, dass es gut ist wenn wir in unserer [...] App die Möglichkeit bieten, dass man eben über sichere Wege kommunizieren kann.)*

Design

Most of the experts believe that the design of a mobile application can affect the user's trust. Expert J gave an example about websites:

> [...] A site that does not give a serious impression, I believe I would trust less [in this one] than in a site that manages my data well [...]
> *([...]Eine Seite, die keinen seriösen Eindruck macht, [in die] habe ich glaube ich auch weniger Vertrauen darin, dass die meine Daten gut verwalten [...])*

Expert H argued:

> If the user-interface is really bad, then other things might also not be of high quality [...]
> *(Wenn amal das User-Interface scho sehr schlecht ist, dann wird wahrscheinlich dahinter das a ned von hoher Qualität sein [...])*

Expert F was also of this opinion:

> If something [...] is technically well developed, then [...] it is in my opinion more trustworthy.
> *(Wenn was [...] handwerklich gscheit umgesetzt ist, dann [...] ist des meiner Meinung nach gleich glaubenswürdiger.)*

Benefit for the user

Apart from all these arguments of how to increase trust, some experts brought forward the argument that often the benefit has to be greater than the disadvantage. Then users may use an application even if they do not think that it is trustworthy. Expert A explained the benefit for users:

> [...] the individual benefit of an application has to be greater than the subjectively perceived risk or the potential of the problem which comes with the collection of data [...]
> *([...] der individuelle Nutzen von so einer Applikation muss eben des subjektiv wahrgenommene Risiko oder das Problempotential was sich mit dieser Datensammlung mit sich bringt bei weitem überwiegen [...])*

Expert D explained the following about the majority of the users:

> I believe that the functionality is more important than privacy and security concerns.
> *(Ich glaub da geht die Funktionalität über Datenschutz und Sicherheitsbedenken.)*

Therefore, in addition to all the efforts to develop a trustful mobile application, the application should have very good functionality and features.

5.3 Summary

The interviews with the 10 experts yield interesting ideas and methods to increase trust in community-based mobile applications. Rating systems with the possibility to describe the user's evaluation in more detail was an aspect which many experts generally agreed on.

Presenting information, like one's real-name or a profile image can, according to some experts, also improve the trust in social networks. Some experts also mentioned a friendship or following system to create trust.

Security is often seen as a base condition for generating trust, but it was also pointed out that these security mechanisms have to be mediated to the user.

Most of the experts claimed that privacy is an important factor for generating trust. Information has to be handled with care and should, like the security mechanisms, be explained to the user in, for example, privacy policies. When privacy works well in a system and the user is not afraid of sharing some information, this information can help to increase trust again.

When talking about open source most of the experts agreed that it increases trust. But it has to be considered that all experts have a technical point of view and know what open source means. For users without technical background this assumption might not comply.

Advertisements divided the opinions of the experts and no clear statement can be given. Some said that it decreases their trust, others think that it has no effect on them. Perhaps this is a subjective perception that also depends on the number, size and type of advertisement.

Communication was only mentioned by a few experts. But I think that this is because many of them took this for granted when talking about community platforms and did not even think about it. However, I think that communication is important to increase trust between users because it can give the user an impression of the other user.

Design was often mentioned as a factor that influences trust. Most of the experts derived from the design of a mobile application how the rest of the application was developed.

In the interviews some experts described that users often use an application if the benefits of using an application are greater than the disadvantages. Therefore, when developing an application it should be considered that the feature has to convince the user. But of course this should not be the only aspect taken into consideration.

CHAPTER 6

Survey

In the interviews I realized that trust is often perceived differently and depends on the user who uses the application. It can depend on many different factors, for example on the user's technical background. Users with a technical background might consider things as trustful that other users might not. In the interviews I only asked experts with such a technical background. The number of these people asked were very limited because of the qualitative interviews.Therefore, it would also be interesting to get a more general result - a result from a bigger group of users. A result from users, who do not necessarily have a technical background.
For that reason, I designed an online-survey with a self-administered questionnaire [Fin03a, p. 22]. With this I want to explore what the majority of users think about the role of trust in social networks and mobile applications.

In 'Information about the Survey' I explain in general how the questionnaire was created and how it was published. The major section of this chapter is 'Results of the Survey'. In this section I present all the results of the questionnaire which are summarized in 'Summary'.

6.1 Information about the Survey

The questionnaire was a self-administered questionnaire [Fin03a, p. 22] and was accessible online. It contained only closed-ended questions as explained in [LFH10, p. 112] and one open-ended question to give the attending people the possibility to write some comment.
The questionnaire was created with Google Forms which is part of the Google Drive platform[1]. With the help of Google Forms questionnaires can be easily created with an editor. It was published on different kinds of channels. Facebook, e-mails, forums and one comment on an article on a newspaper platform were used to make the questionnaire public. The questionnaire can be found in the Appendix (figures A.10,A.11, A.12 and A.13).

[1] see for more details `http://www.google.com/drive/apps.html`

In the questionnaire I asked if the participants had any special education in computer science, like studying software engineering. I refer to users who had such an educational background as 'technical participants' in this chapter.

6.2 Results of the Survey

I asked the participants different kinds of questions about the core elements for this thesis: about trust in social networks and mobile applications. The results are summarized in the following subsections: 'General Information about the Participants', 'Results about Social Networks' and 'Results about Mobile Applications'.

General Information about the Participants

The questionnaire was answered 152 times. 53,29% of the participants were women and 46,71% were men (see figure A.8 in 'Appendix'). Most of the participants had a smartphone: 78,29% of them had a smartphone at the current time (see figure A.9 in 'Appendix').

Figure 6.1 shows the age of the participants. Most of them were between 21 and 30 years old. This figure also shows the distribution of people with computer science education in relation to their age. 73,03% of all participants were non-technical participants. This means that they had no special education in computer science.

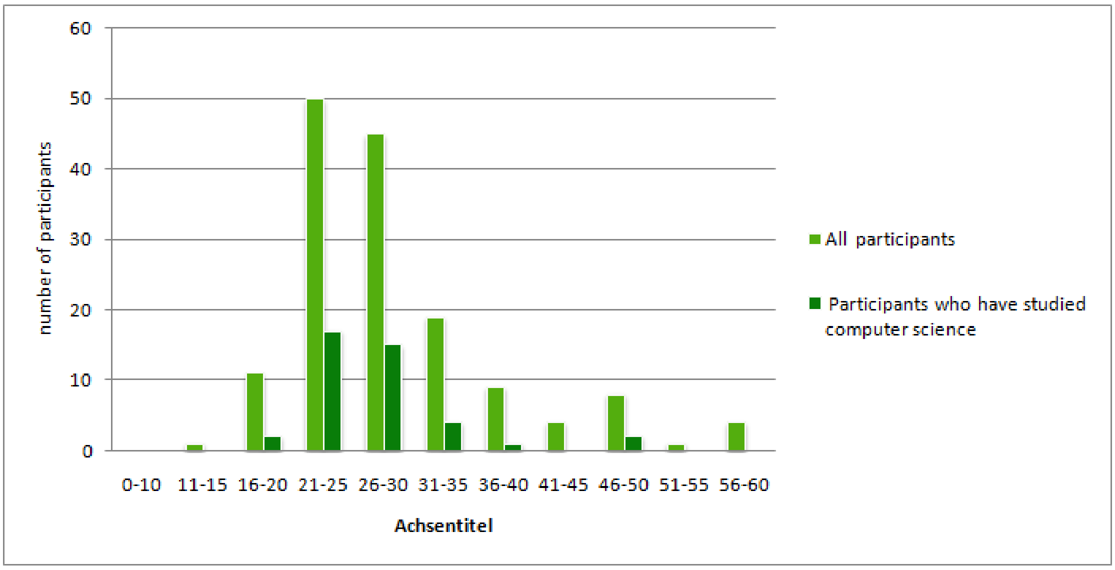


Figure 6.1: Questionnaire distribution by age and attendance of participants with computer science education.

I asked the participants about their knowledge of technology on a range between 1 and 5. 1 is the lowest and 5 the highest grade that can be chosen. 3,29% of the participants chose ’1’, 12,5% chose ’2’, 28,29% chose ’3’, 34,87% chose ’4’ and 21,05% chose ’5’ (see figure 6.2).

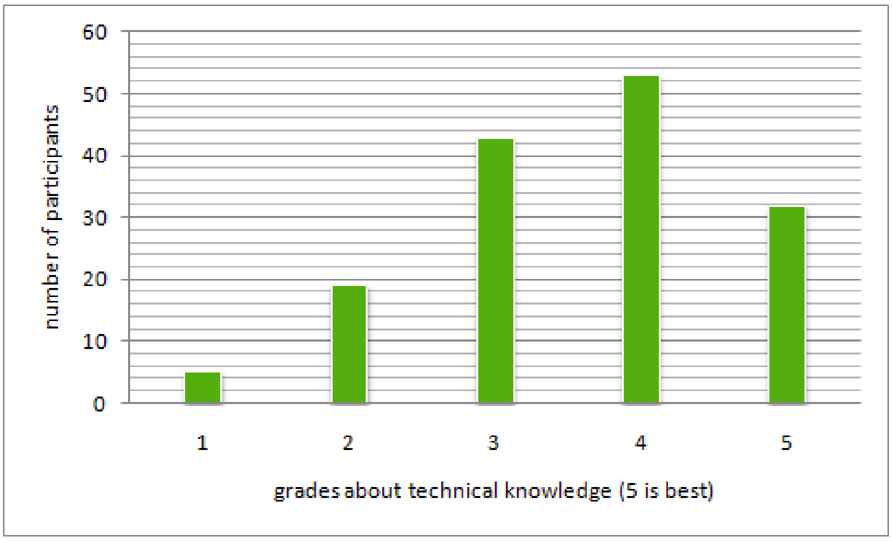


Figure 6.2: Questionnaire distribution about technical knowledge.

Results about Social Networks

One aim of this questionnaire was to see which mechanisms influence the trust of the majority of the users of social networks. I asked questions which evolved during my practical part, literature research and the interviews, but also questions about mechanisms that already exist (partly) in some social networks.

Information about the User Himself/Herself

One of these mechanisms, which is already used in some social networks, is the use of real-names. A real-name means that the user has to or should use his/her real name in the social network instead of some fictional user name. In the questionnaire I asked how real-names influence their trust in social networks or in their users. The results of this question can be found in figure 6.3. Most of the participants stated that it has a positive influence on trust: 56,58% were of the opinion that it influences their trust in the social networks or in their users slightly or even more.

In most social networks, one has the possibility to add a picture of oneself. Like for real-names, the participants tended to trust the social network or their users more if they used profile images: 59,87% of them stated that it increases trust slightly or more (see figure 6.4).

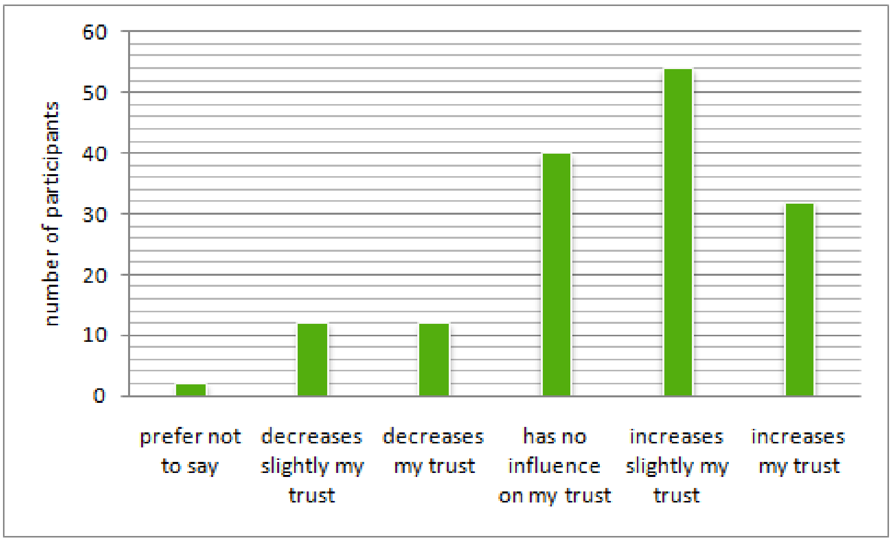


Figure 6.3: Results of the questionnaire about the influence of trust on social networks because of real-names.

An interesting result of the analysis of this data was that many women were of the opinion that pictures have a positive effect: 55,56% of them stated that profile images are a slight factor for increasing trust (men: 30,99%) and 14,81% stated that it increases their trust into the network or the user (men: 16,9%).
Another interesting result was that there was also a big difference between technical participants and non-technical participants. While only 29,73% of the non-technical participants stated that profile images have no influence on them, most of the the technical participants stated that they have no influence on their trust (41,46%). Therefore, profile images seem to have a different influence on different groups of people.

Apart from real-names and images, the user often has the possibility to show other information about himself/herself. This could be any kind of information, for example: his/her address, where he/she works, which food he/she likes, etc. 50% of the participants stated that it slightly increases their trust in others (see figure 6.5).

A possibility to increase trust would be to check the identity of the users (see figure 6.6). This would be much work and would evoke privacy concerns. However, most of the users were of the opinion that it would increase their trust (slightly: 28,29%, more: 31,58%). Only 18,42% stated that it had no effect and 16,44% stated that it would decrease their trust slightly or more.

Due to my findings, I reckon that users in general trust more in another user if he/she knows more about him/her. This is true for real-names, profile images, private information and proven identity. Over 50% of the participants were of the opinion that such things increase trust.

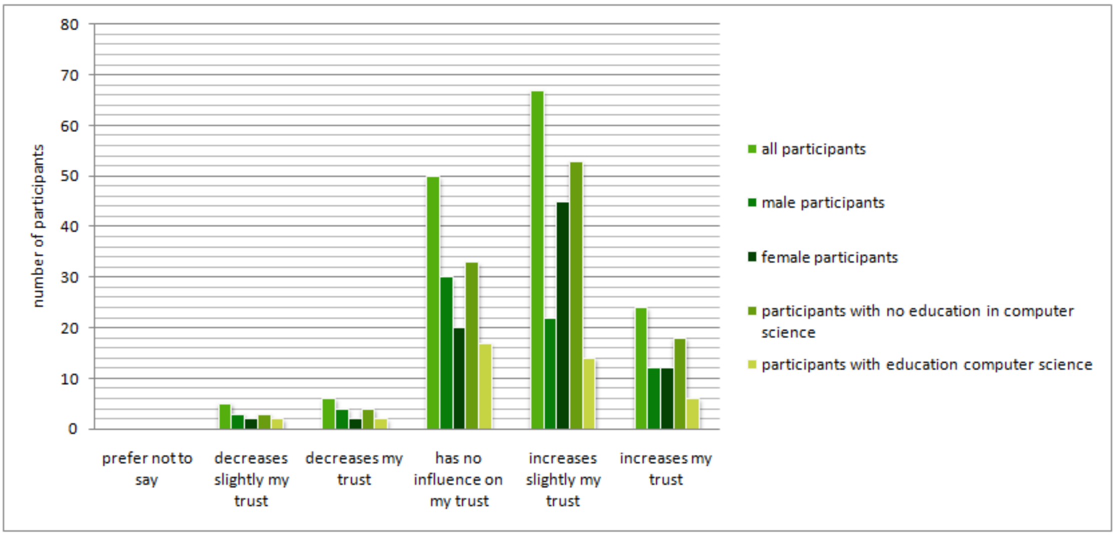


Figure 6.4: Results of the questionnaire about the influence of trust on users of social networks because of profile images.

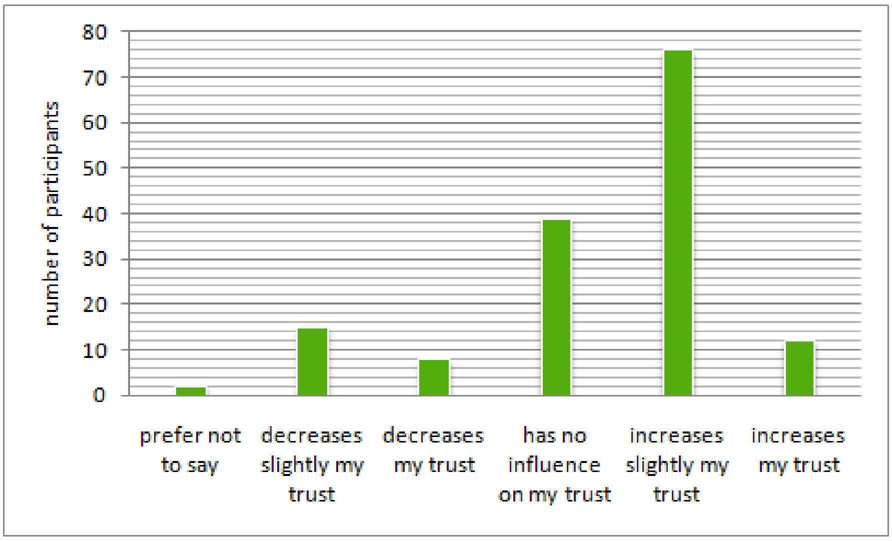


Figure 6.5: Results of the questionnaire about the influence of trust on users of social networks because of private information.

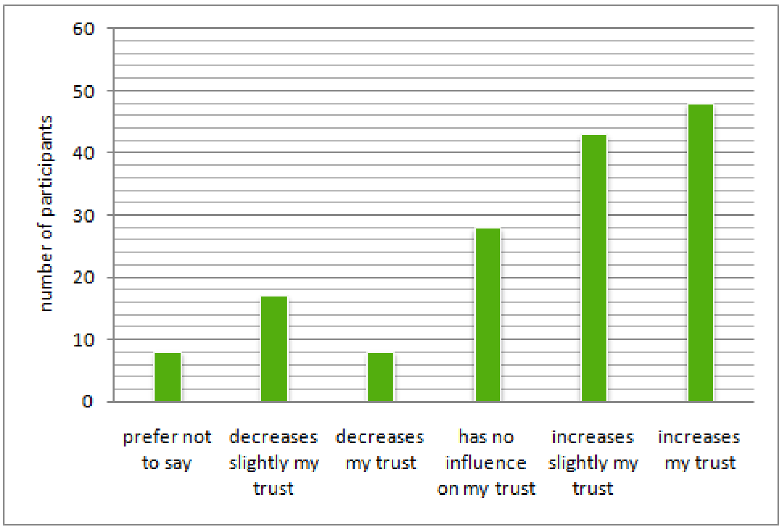


Figure 6.6: Results of the questionnaire about the influence of trust on users of social networks because of proven identities.

Context Information about the User Described by Others

Another technique which is already used, is to describe one user by his/her context: ratings about the user and his/her content and his/her history of interactions.

Figure 6.7 shows that ratings about users seem to effect users differently. 32,24% of all the participants stated that it has no influence on their trust, but exactly the same number of users stated that it has a slight influence on them. But when summarizing the positive effect on trust, it outvalues the neutral opinion: 53,29%.

An interesting result of the questionnaire is that most of the participants stated that a rating about the activities of users has no influence on their trust on them (see figure 6.8). 42,76% were of this neutral opinion. The rest of the users were mostly of the opinion that it increases their trust into the others slightly (25%) or more (13,82%) .

Another possibility to make the user better known in this social network is to display some history of the user (see figure 6.9). For example, in Open-Share-It, the user could be shown how many foodbaskets another user has already offered or taken.
Most of the participants agreed that it slightly increases their trust (36,84%) and some even agreed that it increases their trust more (20,39%).

So, according to these results, information about the user like ratings or his/her history can increase the trust in him/her. But the results were not as clear as the results from ’Information about the User Himself/Herself’.

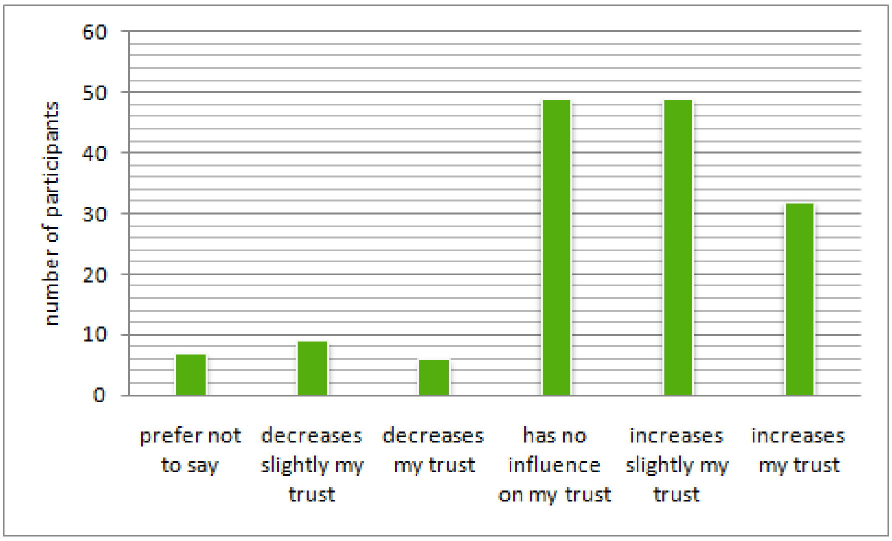


Figure 6.7: Results of the questionnaire about the influence of trust on users of social networks because of ratings about him/her.

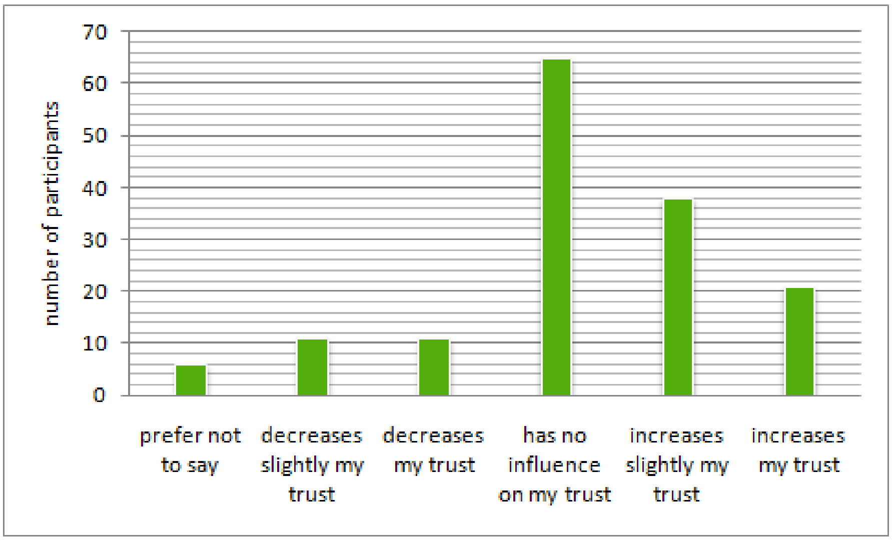


Figure 6.8: Results of the questionnaire about the influence of trust on users of social networks because of ratings about his/her activities.

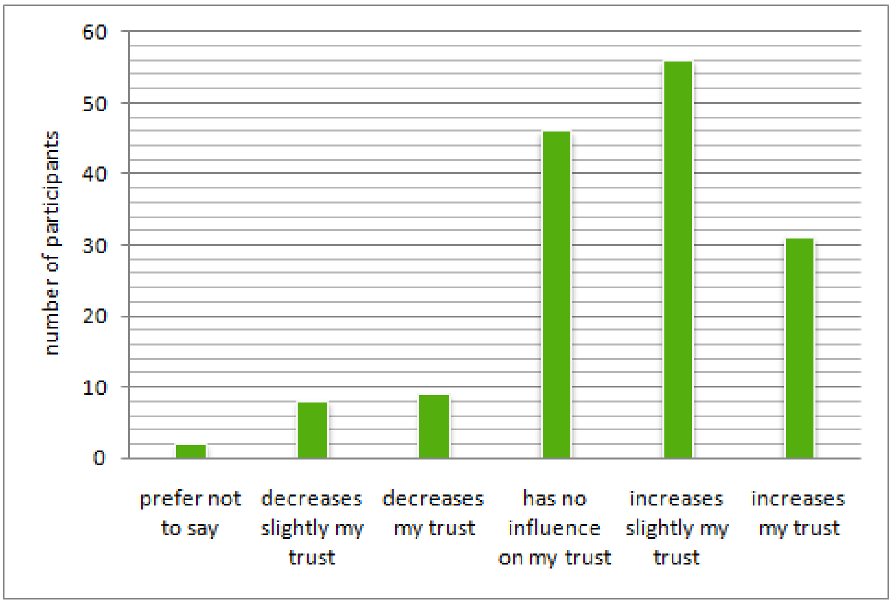


Figure 6.9: Results of the questionnaire about the influence of trust on social networks because of user's history in this social network.

Communication, Button to Report Abuse and Advertisement

In the questionnaire I asked the participants questions about factors that could have an influence on their trust. One question was about communication in social networks. I asked this question because in the interviews communication was pointed out by some of the experts. In the questionnaire 34,87% of the participants stated that communication has no influence, while 37,5% stated that is has a slight and 22,37% claimed to be influenced even more in their trust relationship (see figure 6.10). So, more than half of the participants think that communication influences the trust between users.

Often, on websites where users can publish some sort of content, a button to report abuse is used to keep the content 'clean' and correct. If users think that the content is scandalous, inappropriately used, or the user has any other kind of claim about the content, he/she can press the button and may give some comment so that the provider of the platform can easily check if the content is correct or not.
Similar to the idea of communication, the majority think that it has a slight(34,87%) or stronger influence (38,82%) on the trust in other users or in the social network (see figure 6.11). In this questionnaire women even tend to trust more in such a mechanism: 35,8% of them stated that it slightly increases their trust (in comparison, only 33,8% of the men asked thought so) and even 45,68% of the women stated that it has (more) influence on their trust in social networks (only 30,99% of the men stated so).

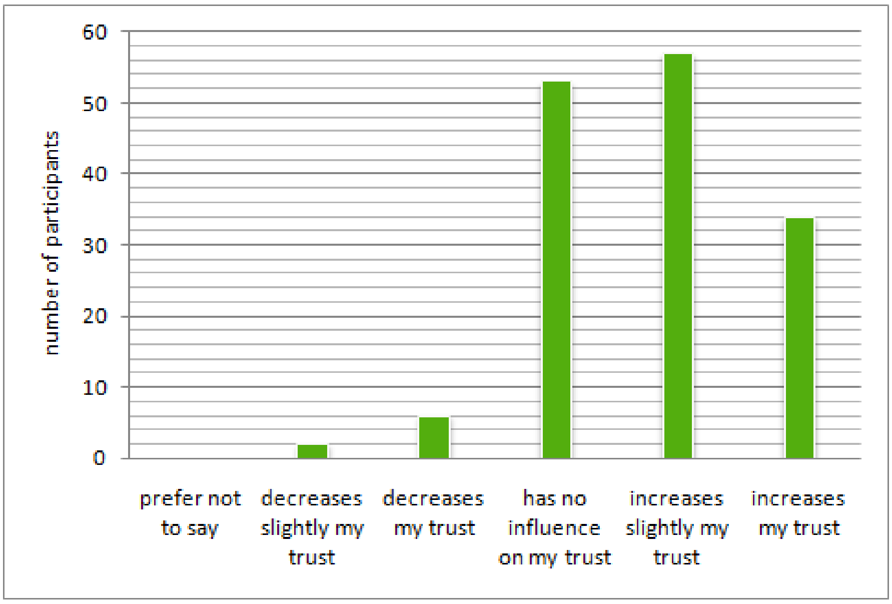


Figure 6.10: Results of the questionnaire about the influence of trust on social networks because of communicating with the other user.

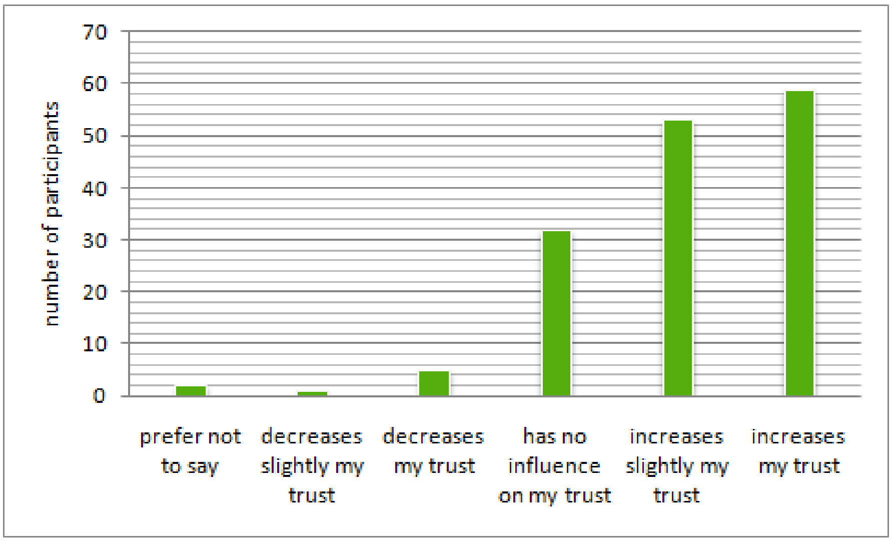


Figure 6.11: Results of the questionnaire about the influence of trust on social networks because of a button to report abuse.

The last question regarding social networks was about advertisements. As one can see in figure 6.12 most participants think that advertisements decrease their trust (slightly: 25,66%, more: 42,76%). 25% of the participants stated that it has no relevance for their trust in the social network. According to that, the majority think that it has a negative influence on their trust.

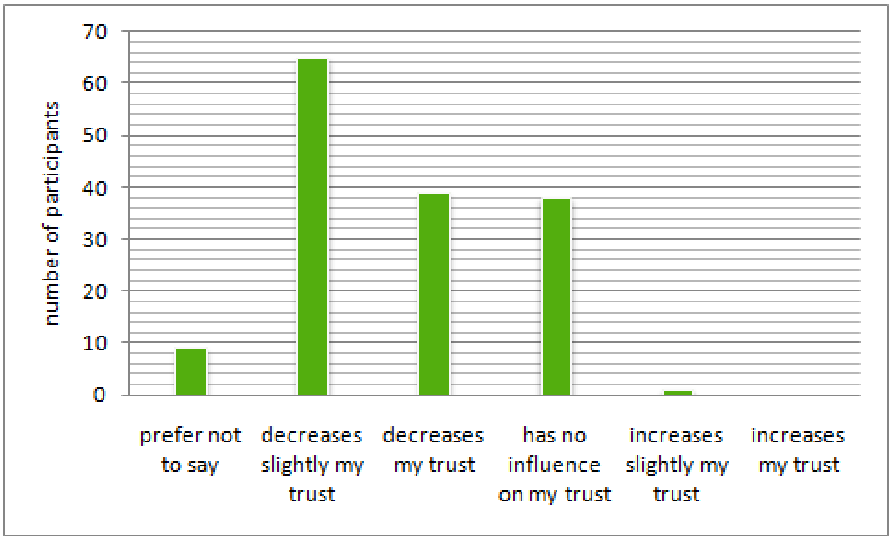


Figure 6.12: Results of the questionnaire about the influence of trust on social networks because of advertisement.

Results about Mobile Applications

Apart from questions about trust in social networks I also concentrated on questions about mobile applications. This time I also asked questions which evolved during the development of the Open-Share-It project, literature research and the interviews.

Design

One of the first things a user recognizes when using a mobile application is its design. It can be structured, familiar, creative and much more. Some designs appeal to one, others do not. So it often is a very personal opinion whether one likes the appearance of an application or not. I asked the participants if design they like and design they do not like has an influence on their trust in the mobile application.
In figure 6.13 one can see that design which a user likes can positively influence his/her trust (increase slightly: 40,79%, increase more: 13,82%) and design he/she does not like can negatively influence his/her trust (decrease slightly: 21,05%, decrease more: 31,58%). However, in both cases more than 30% of the participants say that it has no influence on their trust (design you like:36,84%, design you do not like:38,82%).
Another interesting observation is that in this questionnaire men find design more important for trusting than women (in comparison: 46,48% of the men stated that design they like can increase their trust slightly, while only 35,8% of the women were of this opinion). Also, more non-technical participants stated that design affects their trust in mobile applications than technical participants do (46,85% of the non-technical participants stated that design they like increases their trust slightly. Only 24,39% of the technical participants stated the same).

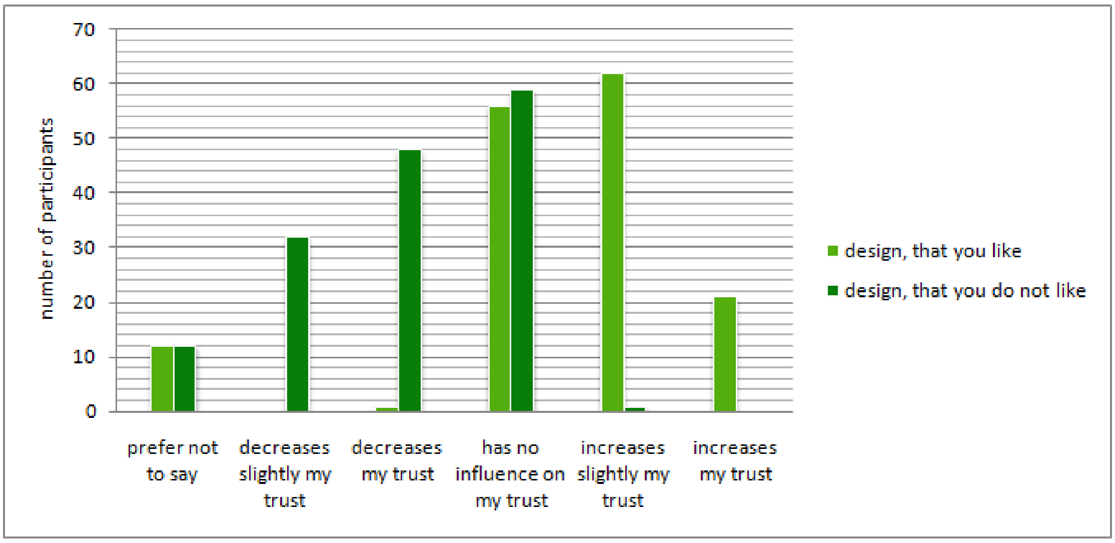


Figure 6.13: Results of the questionnaire about the influence of trust on mobile applications because of design one likes or does not like.

Security and Privacy

Security in general is not quite easy to see in mobile applications. Therefore, I asked if security activities that are communicated to the user have an influence on their trust in the mobile application. Figure 6.14 gives a clear picture: 80,92% of the participants stated that it increases their trust in the mobile application slightly or more.

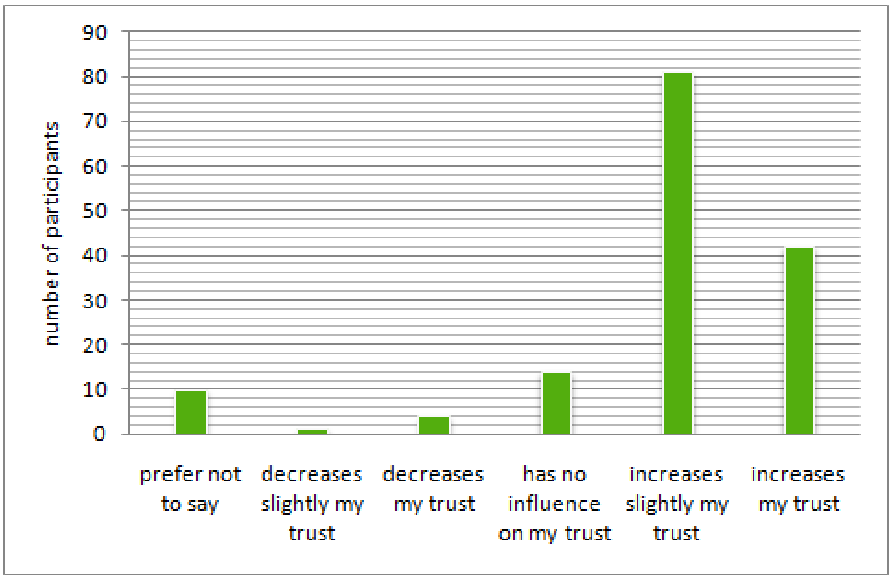


Figure 6.14: Results of the questionnaire about the influence of trust on mobile applications because of communicated security.

One possibility to make security considerations public is to use security policies (see figure 6.15). The majority of the participants said that it slightly increases their trust (42,11%). But fewer participants, in comparison to security concerns, stated that it increases their trust slightly or more: 50,66% in total. Consequently, one might assume that security is important to increase trust, but policies might not be the best solution to express the provider's effort in this area.
But it is important to note that between 19,08% and 19,74% of the participants answered 'prefer not to say' for the question about security policies, privacy policies and open source projects. Especially non-technical participants used this answering option: 24,32% of them stated so about security policies. Therefore, I assume that these terms are not very well known and because of that, many chose this option. Perhaps the result would conform more to the results of communicated security if more users knew these terms. Nevertheless, even if some would have chosen a positive influence option, the result is less clear than the result about communicated security.

The results for privacy policies are similar to the ones about security policies, as can be seen in figure 6.15 and therefore, they do not need further explanation.

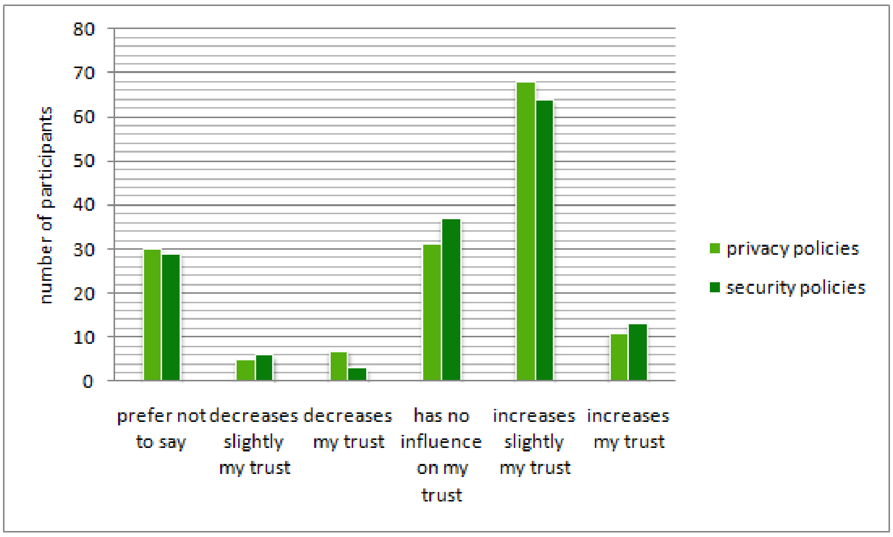


Figure 6.15: Results of the questionnaire about the influence of trust on mobile applications because of privacy and security policies.

Another way of trying to ensure and communicate privacy and security is by using certificates. In mobile applications they are not very common, but especially in webshops, these certificates seem to be a good mechanism to create trust. In figure 6.16 one can see that the majority thinks that it can increase their trust in mobile applications: 40,79% stated that it would slightly increase their trust, 21,71% said that it increases their trust even more. In this case, technical participants were even more often of the opinion that it would increase their trust than non-technical participants (in comparison: 48,78% of the technical and 37,84% of the non-technical participants stated that it increases their trust slightly. 26,83% of the technical participants stated that it increases their trust (more) while only 19,82% of the non-technical participants had the same opinion).
Even if they are not very common today, according to the results, certificates like TRUSTe[2] could increase the user's trust in the application.

I asked the participants about the usage of their resources by a mobile application. Often, mobile applications want access to photos, the users' contacts, addresses and much more. As figure 6.17 shows, users in general would trust more in an application where they know what is happening with their data than in an application where the users' data are used without any further information. Especially technical participants think that it decreases their trust if they have no further information about what is happening with the resources (decreases more: 92,68%). In comparison, technical participants are rather of the opinion that if the provider of an application provided more information about the use of the users' data, it would slightly increase their trust

[2] http://www.truste.com/

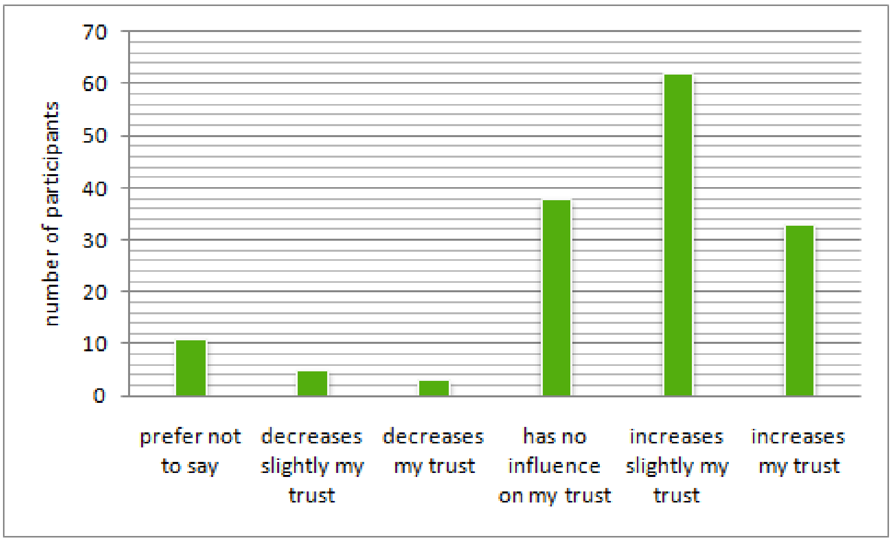


Figure 6.16: Results of the questionnaire about the influence of trust on mobile applications because of certificates.

(technical participants:46,34% non-technical participants:17,12%).
In general, it can help if the user knows why he/she has to give some personal information. Still, even if the provider explains why he/she needs some of the data, he/she should be careful about asking for information or resources because even then 46,72% of the participants stated that it decreases his/her trust in the mobile application slightly or more.

One great benefit of using smartphones is that the user has the possibility to use GPS. With GPS a mobile application can locate the user, present his/her position on a map, filter or sort results dependent on the users' location etc.
According to the results, GPS information can decrease the trust in the mobile application. 27,63% of the participants were of the opinion that it slightly decreases their trust in the mobile application and even 38,16% were of the opinion that is decreases their trust even more.
According to the results, the use of GPS information has no great effect on the trust for other users. Both results can be seen in figure 6.18.

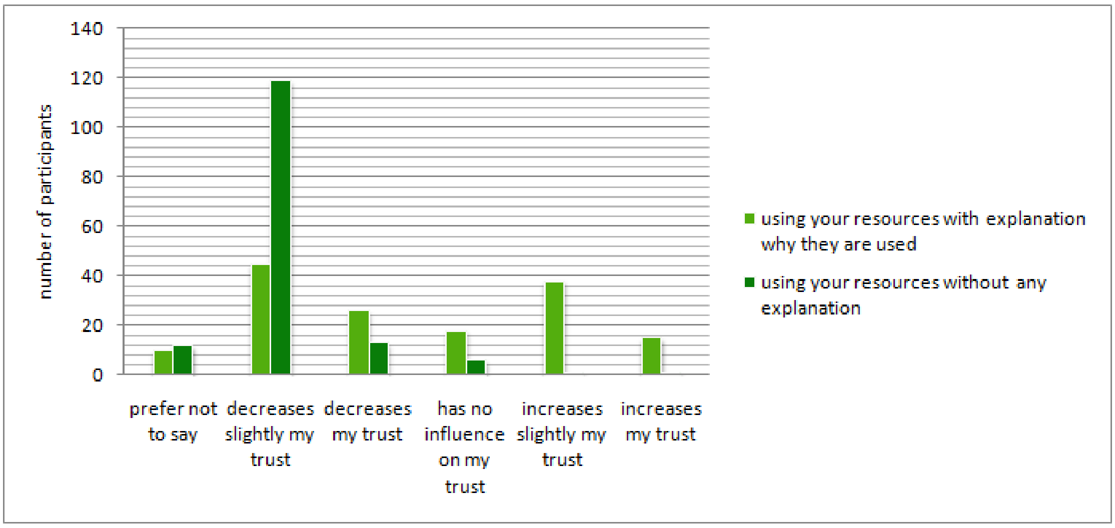


Figure 6.17: Results of the questionnaire about the influence of trust on mobile applications because of using users' resources.

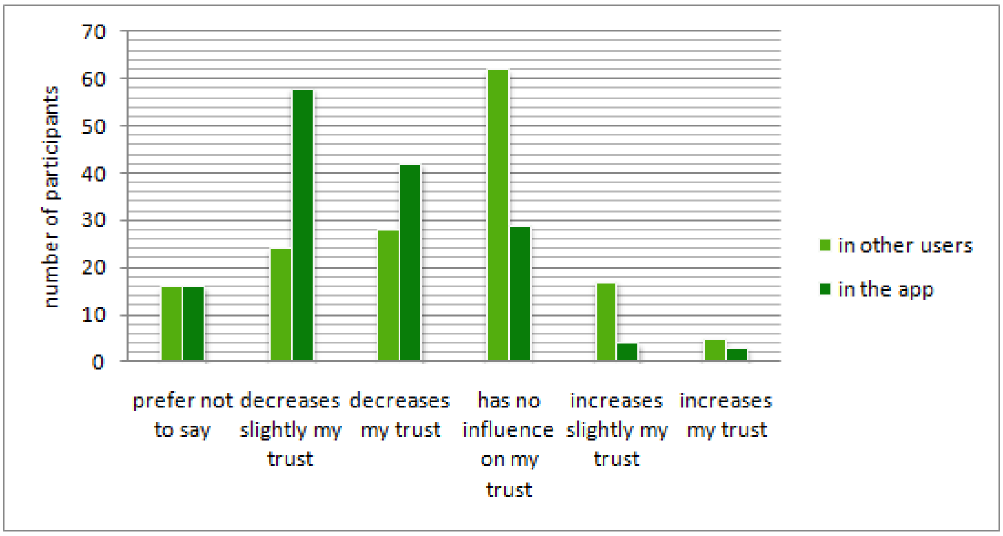


Figure 6.18: Results of the questionnaire about the influence of trust on mobile applications because of using GPS-data.

Advertisement, Open Source and Being always Online

In this last part I explain the results of advertisement, open source projects and the feature of always being online with the mobile application.

As expected, advertisements in the context of mobile applications seem to have similar results as for social networks (see figure 6.19). The result could have been different because advertising in mobile applications is, in my opinion, differently used than in social networks. Anyhow, 23,68% of the participants were of the opinion that it slightly decreases their trust and even 46,05% stated that it has a more negative effect on their trust. So, even in mobile applications, developers should keep in mind that advertisement can influence the trust of their users.

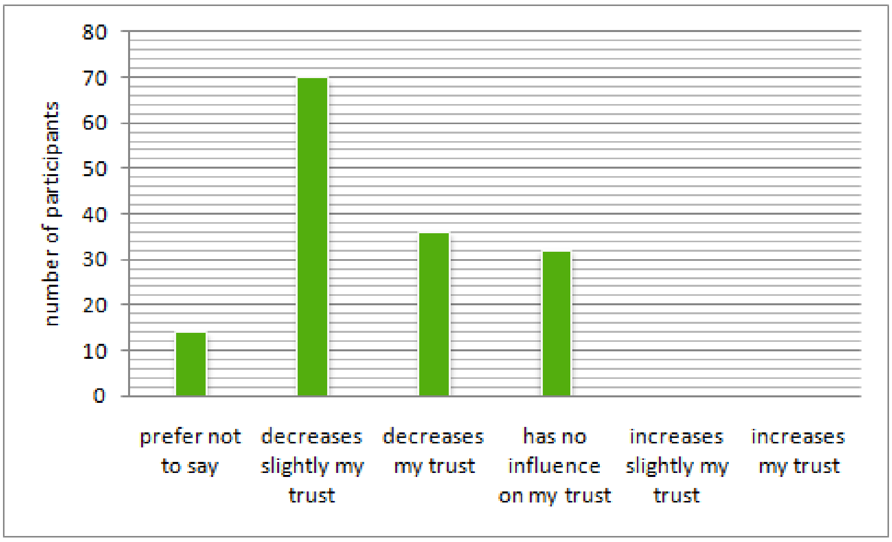


Figure 6.19: Results of the questionnaire about the influence of trust on mobile applications because of using advertisement.

Open source projects are frequently used in software development and help to advance technology. Open-Share-It is an example for an open source project. It can be adopted by anyone so that anyone who wants (and has the resources) can easily create his own Sharing-platform.
Figure 6.20 shows that in total the majority found that a mobile application which is developed as an open source project slightly increases their trust or even more regarding that. But, as already mentioned for security and privacy policies, this question has one of the highest rate for ’prefer not to say’ (19,74% of all participants). While 48,78% of the technical participants stated that it increases their trust, only 14,41% of the non-technical participants were of the same opinion. I think that this high rate of choosing the option ’prefer not to say’ is due to the fact that the term open source is not very well known by non-technical participants.

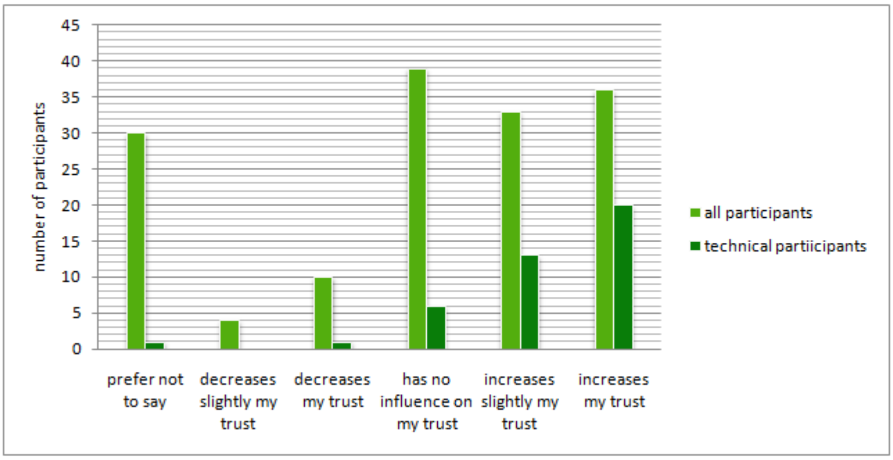


Figure 6.20: Results of the questionnaire about the influence of trust on mobile applications because it is an open source project.

Many applications use a concept of being always online. For example, in Facebook you have the possibility to close the application without logging out. Then you can receive notifications and easily start the application without entering your username and password again.
In the participants' opinion this can decrease the trust in the mobile application (see figure 6.21). 23,68% of them stated that it slightly decreases and 40,13% claimed that it decreases their trust more in the mobile application. Especially technical participants were of this opinion (slightly: 24,39%, more: 48,78%).

Comments from Participants

The participants had the possibility to give a comment at the end of the questionnaire. These are the most important results:

Some participants pointed out that they had difficulties in answering some of my questions. One participant explained that it was difficult to give a general answer because it often depends on several other things as well. For example, one person explained that it is difficult to say whether advertising influences one's trust in a social network because it depends very much on the type of advertisement and what it is about. Another person would have liked to have a clear definition of trust and another one stated that the last three question could have been more precise.

Some participants explained which factors have a great influence on their trust. One person said that communication is very important to him/her, another participant explained that in Foodshar-

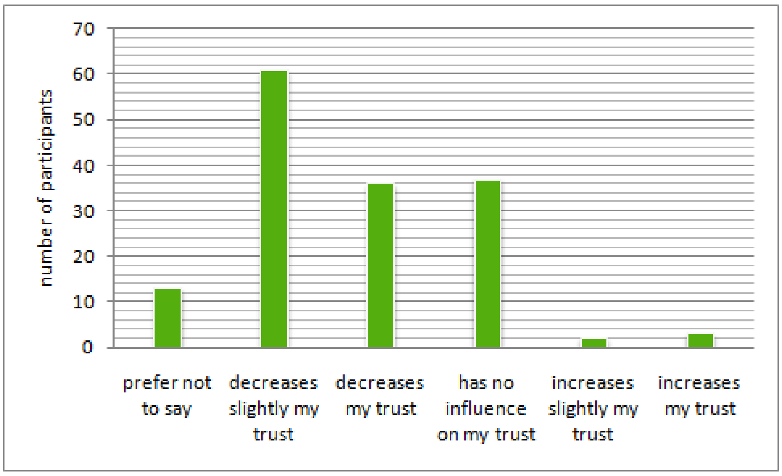


Figure 6.21: Results of the questionnaire about the influence of trust on mobile applications because of being always online.

ing addresses should not automatically be shared between the requestor and the provider of a foodbasket - the users should be able to choose this option.

6.3 Summary

It was very interesting to carry out this questionnaire. It showed which mechanisms influence the majority of people in their trust in other users, the social network or the mobile application. So, what general results can I report after analysing the data?

First of all, regarding social networks, most of the participants were of the opinion that information about the user, like his/her name, his/her account picture and other information, can increase trust. The same goes for proven identities: most participants thought that it would increase their trust if the users in social networks were verified (for example by the platform).

Second, information about the user described by others (ratings) and his/her activities (his/her history) can also increase one's trust in the user. However, I was surprised that the result was not an unambiguous assignment as I had expected.

Third, according to the results of the questionnaire, a button to report abuse and the possibility to communicate in social networks can have a positive effect on the trust in the social network. Advertisements, regardless if used in social networks or in mobile applications, decreased most of the participants' trust.

According to the results, the design of a mobile application can influence the trust of a user in the application. Design he/she likes can increase his/her trust. Design that he/she does not like can decrease the trust regarding the mobile application.

Over 80% of the participants answered that security (communicated by the provider) can slightly increase one's trust in the application. This is the most definite result in general. In my opinion it expresses the user's need to get assured that his/her data is protected. This is also reflected in the result about security and privacy policies: they can increase the user's trust in the mobile application.

The use of resources, like contacts, images or GPS data can, on the one hand, increase the user's trust in other users of social networks, but on the other hand it can decrease the trust of a user in a mobile application. Therefore, it is important to ask only for data that is really needed and it is important to explain why this data is needed.

Another result is that certificates, as already used in the e-commerce area, can increase the trust of a user in the mobile application. The concept of always being logged in, in an application can decrease the trust of the user in an application. I assume that this is because users might fear that the application collects data (e.g. GPS), about them. Therefore, I think it is a good solution not to hide the log out button because otherwise users might trust less in the application.

Last but not least, I want to mention the open source projects for mobile applications. As expected, technical participants were of the opinion that it increases their trust. In general, participants had a similar opinion, but many claimed that it had no influence on them or chose the option 'prefer not to say'. If open source projects were understood by more people (especially non-technical participants), I think more users would say that it increases their trust.

Apart from all these results, I also found some sex specific differences as well as differences in attitude due to different educational backgrounds. Of course, trust is subjective and means something different to each of us. Nevertheless, this survey showed some important facts that developers of a (community-based) mobile application should keep in mind.

CHAPTER 7

Guidelines for Trustful Mobile Applications

Trust is a very complex, subjective and vague term that depends on the context and is not easy to define and to develop. Especially in quite new areas (compared to other technologies), like smartphones and social networks, trust still needs to be explored much more. In these areas trust is especially important and should be handled with care.

In this thesis, I investigated how trust between users in a social network application for a smartphone can be enhanced by the application as well as how the user's trust can be increased in such an application. I did literature research, held interviews with experts and carried out a survey to find out more about trust-relating factors.
In this chapter I synthesize all the results from the previous chapters and present guidelines for this topic. Of course, I do not claim that this list is complete, but it should give the reader a good overview and a starting point to increase trust in such applications.
Some of the results may also be practicable in other areas and are not restricted to mobile applications that support a social network. Because of that, I hope that my advice will be taken into account and has an influence in other areas as well.

7.1 Guidelines

In the following the guidelines are presented to enhance trust between the users in community-based mobile applications as well as the user's trust in such a mobile application.

1. Use rating systems for users and their actions

Rating systems should be used in which users can rate other users or their activities with some sort of grading scheme (for example 1 to 5 stars) and they should be given the opportunity to

comment on their rating. These ratings can be summarized and an average result can be displayed about the user or his/her activities.
With this mechanism, other members get further information about the user and his/her activities. It can help the user to create a basic trust in the other person and can be one of the first steps in evolving trust.

This guideline results from different sources. It is a result from my experiences of developing the Open-Share-It project. I also gained this idea from my literature research (see 'Reputation Aspects') and from experts (see 'Ratings'). The survey showed that trust can be increased by using rating systems (see 'Context Information about the User Described by Others').

2. Let the users communicate

A social network should provide a communication channel in which users can chat without sharing private information like e-mail address or phone number. People can discern important information from communicating with another person. It can enhance the trust between these users.

This piece of advice results from the interviews I held (see 'Communication'). We also thought about integrating it in the Open-Share-It project and the survey also showed that the users want that (see 'Communication, Button to Report Abuse and Advertisement').

3. Use following or friendship mechanism to make trust transitive

With a friendship or following mechanism users may trust other users more because they might for example be a friend of a user's friend. Some users may use this transitive relation to trust users who they would not trust otherwise (because they do not know them or only know very little about them).

Especially a friendship mechanism could provide such transitive effects. In following system it may depend on the semantic of following someone. For example, following systems with the meaning of following someone because he/she provides interesting or funny content may not influence the other user's trust. But a following system for the Open-Share-It platform, where users can follow others because they are interested in their foodbaskets, can have a transitive effect. In such systems, following one person often means that the followed person does not need to give his/her agreement. Therefore, friendship systems may be the better way to achieve this transitive effect.

The following or friendship mechanism was mentioned in the interviews by experts A and J (see 'Friendship or Following Systems') and was discussed as a feature for the Open-Share-It project.

4. Present voluntarily given information to other users

Information about the user can increase the trust-relationship between users. A real name or a picture can help to get an idea of the other user. Of course, only data should be presented which the user agrees with (except in special cases).
Apart from this information, information about the user in this social network can also be very helpful. Information of his/her past activities can help other users to enhance trust. Ratings, as already mentioned, are useful in this case and can be helpful to describe a user.

This was a much-discussed topic during the interviews (see 'Information'). The people taking part in the survey also considered this as essential (see 'Information about the User Himself/Herself'). In the Open-Share-It project the presentation of information is an important concern.

5. Present voluntarily given information carefully

Even if it is attractive to use all the pieces of information in the mobile application, the developers should always keep in mind to treat the data securely. It is important that information does not get lost or modified or added without the user's approval. It is also very important that the data has different access levels. Some data may only be shared with friends, others should be private. The social network provider should always take care about these levels and ensure to stick to them.

Handling the presented data with care is implicitly mentioned in my literature findings, in the interviews as well as in the survey. In the chapter 'Related Work' I explained that the data should be cared with respect, listed security as one of the technical aspects and described the 'history of acting well'. It was explained by expert J in the interviews (see 'Information') and had been asked implicit in the survey.

6. Let the user give you feedback

A button to report abuse can increase the trust of the members of a social network on a mobile application. It is also a good mechanism to find incorrect or improper content quickly. Of course, the user should also have the possibility to contact the provider of an application by other means (e.g.: contact form, service-line). So he/she can also report abuse, bugs or give feedback to enhance the user's satisfaction.

A button to report abuse is common on websites and has already been discussed when developing of the Open-Share-It project. Most of the participants of the survey were of the opinion that such a button could increase trust in the system (see 'Communication, Button to Report Abuse and Advertisement').

7. Let the user control his/her data

The user should always have the control over his/her data. If he/she can choose by himself/herself what information he/she provides, it can increase his/her trust in the mobile application. For example, an application should ask the user if he/she wants to send GPS data about his/her location. The user should always have the possibility to change his/her data or even to delete it (if the data is not required).
The user's data should by default not be shared with third-parties. The data should only be transmitted to others if the user agrees with that. Newsletters or other pieces of information that could annoy the user should by default not be enabled.

This guideline mostly results from my literature research (see 'Privacy Aspects'), the survey (see 'Security and Privacy') and is implemented in Open-Share-It.

8. Explain why you need the information

Before accessing data, it can help the user's trust in the application if the mobile application explains the user why some data is required from him/her. With this information the user may understand the need to access his/her data and is maybe willing to give this data to the provider.

In the interview expert E claimed that transparency is very important (see 'Privacy') and when analysing the survey I also came to the result that it can increase the user's trust if the user knows why some information is needed from him/her.

9. Avoid location-based data if not needed

The developer of an application should be careful to use location-based data. If a mobile application uses a map where the user's position should be displayed, the user possibly will have no objections to using his/her GPS data. But there are other cases, when the request for one's location is not obvious for the user and that can decrease his/her trust in the mobile application.

Expert J explained that if the application always knows where you are, this can have 'a bad taste' (see 'Privacy'). Most of the participants were of the opinion that the use of the GPS can have a decreasing effect on the application (see 'Security and Privacy').

10. Make your application secure

The application should handle the user's data with care in each process and beyond. Keep in mind that the loss of data might have incredible consequences: the loss of one's reputation, as well as one's trust are only examples of the possible results of that. Use as many security mechanisms as possible, but keep the usability in mind. For example, it may be very secure to use a password with 200 characters - but nobody would use such a system if 200 were required.

This issue was mentioned in all investigations. I came across it in my literature research *(see 'Technical Aspects'), in the interviews (see 'Security') and many participants of the survey strongly agreed that it can increase trust (see 'Security and Privacy').*

11. Present your privacy and security measures

In the development of a mobile application, security should be considered throughout the project. To create trust, it is not enough to develop a secure application and to have as few security gaps as possible. It is also very important to communicate to the users that the software is secure and handles the private information with care.
A possible way to achieve this, is to use privacy and security policies. Other methods, like explaining that the application is secure on the provider's homepage or showing certificates for the mobile application, can also increase the user's trust because his/her perceived security and privacy will be expanded.

Policies, 'perceived security' and 'perceived privacy' are explained in chapter 'Related Work' and discussed in chapter 'Interviews'. Policies and the influence of security and privacy for the users are explored in chapter 'Survey'.

12. Be transparent

Another mechanism to enhance trust is being transparent. A. Korff expresses this in the following way [Kor]: 'Let Your Clients See Your Kitchen'. He explains that it would create trust in a restaurant if the customers had the possibility to see the kitchen - to see behind the stage. In other words: it increases the user's trust in the mobile application and the social network if it is transparent. The provider should explain which data is collected, for which purpose they do so and to whom they are shown.

For example, expert E stated that transparency is important (see 'Privacy'). It was also a concern of the Open-Share-It project and is implicitly asked in the survey (see for example 'Security and Privacy' or 'Advertisement, Open Source and Being always Online').

13. Use open source if it is consistent with your business objectives

Often it is not possible to publish the mobile application as an open source project because of business objectives. But if it is possible, it can increase the user's trust. Especially for users who know the term and prize it highly.

One important way to make the Open-Share-It project transparent was to design it as an open source project. It was also discussed in the interviews (see 'Open Source') and was a result of the survey (see 'Advertisement, Open Source and Being always Online').

14. Be technically convincing

Security can often only be guessed to be implemented in mobile applications and is in many cases not visible. Because of that, it is even more important to be technically convincing so that the user has no doubt about the security of the system and that it works well. Otherwise, this can decrease the user's trust.

This guideline is the result of my literature research (see 'Technical Aspects') and in the interview it was discussed in the context of design (see 'Design').

15. Have a good design and usability

Trust in a mobile application can depend on the design of the software. A mobile application should look professional and should satisfy the user. Processes which are known from other applications can, because of its familiarity, increase the user's trust.

I explained this in my literature research (see 'Presentation Aspects'), in the interviews (see 'Design') as well as in the survey (see 'Design'). In the Open-Share-It project we often discussed the design because the project will be published for two different operating systems. In these operating systems other kinds of interaction mechanisms are used to create familiarity.

16. Have features that really satisfy your users

It may be that users use an application even if it decreases their trust in some way. In this case it is important to compensate it with features that the user really wants to use. Nevertheless, the other mechanisms should not be ignored. But important features can help the developers that their mobile application will be used by users even if they are not convinced in each point.

This advice is a result from the interviews. Experts explained that functionality can be very important (see 'Benefit for the user').

17. Be careful with advertisements

Developers of a mobile application should be careful if using an advertisement. They should carefully decide on the numbers, the size and the type of the advertisement. Depending on the advertisement, it can decrease the user's trust in the application.

Advertisements were discussed in the interviews (see 'Advertisement'). The survey also showed that advertisement can decrease the user's trust in the mobile application (see 'Advertisement, Open Source and Being always Online').

18. Present feedback from users and facts

On the corresponding website or on the mobile application itself it can help to display examples of users and their feedback. For example, for the Open-Share-It platform stories from users using the mobile application and who successfully shared foodbaskets could be presented. Of course, this information can be influenced by the provider of the application, but it can give the user an impression of what happens in this social network.

Another thing that can influence the user’s trust is to show some facts about the social network. For example, the number of users, how many foodbaskets were shared and the average rating for foodbaskets. With these facts the user sees how successful this network is and can imagine what happens if he/she will be a member of it.

In the chapter ’Related Work’ a similar mechanism is discussed for web platforms. Often, mobile applications have a corresponding website so that this technique can be used. But the mechanism can also be adopted to mobile applications in general. This sort of information can also be displayed in the mobile application itself.

19. Create a brand and make it public and likeable

As in many other areas, brands can help to create trust. Brands can be used to transfer trust from itself to the system in which it is used. Therefore, it can be helpful to use an already established brand or to make the brand public. A well-designed, sophisticated and well-known brand can enhance the user’s trust in the mobile application and the social network.

Brands and their impact are outlined in the chapter ’Related Work’. We also discussed much about brand in the Open-Share-It project. The cooperation of Foodsharing with the Open-Share-It project could transfer the trust from the brand to the mobile application.

20. Do not hide log out possibilities

Even if it might be attractive for the application provider to hide the log out possibility, it should be used with care. Hiding the log out button may affect the user’s trust in the application. The feeling of control, as already mentioned, plays an important role once again.

In the Open-Share-It project we discussed different features which the user can use if he/she is logged in or if he/she is not. But it was important not to hide the ’Log Out’ button, because otherwise this can decrease the user’s trust in the application (because it tries to keep the user logged in) as discussed in the survey (see ’Advertisement, Open Source and Being always Online’).

7.2 Summary

I synthesized different aspects and methods which I explored in my literature research, interviews and the survey. The presented methods can be used to increase the user's trust in the community-based mobile application. I also gave several pieces of advice of how trust between users can be forwarded.

It often depends on many different factors and many of them cannot be regarded in this guideline. For example, it also depends on the provider's history. An application can be of good quality, but if the user has already had bad experiences with other products by the same provider, he/she may trust less in the mobile application - even if this one seems to be okay.
Nevertheless, these twenty suggestions can increase the trust in community-based mobile applications and should be considered when developing such an application.

CHAPTER 8

Comparison to the Open-Share-It Project

In the previous chapter I introduced guidelines to enhance trust in community-based mobile applications. One source for the creation of these guidelines was the experiences I gained when developing such an application: the Open-Share-It project.
In this chapter I compare the results from the guidelines with the current state of the Open-Share-It project. Some methods explained in the guidelines are implemented - others are not. The reasons for this are also explained in this chapter.

8.1 Results of the Comparison

The Open-Share-It project was developed with a special focus on trust from the beginning on. Despite that, not all the results from chapter 'Guidelines for Trustful Mobile Applications' could be implemented at the current state of the development process. Table 8.1 shows the results of the comparison of the guidelines and the Open-Share-It project.

First of all, due to problems of the collaboration with Foodsharing and due to lack of time the mobile application does not support all features which are destined for the first version of this. One of these features is the rating system. At the current version of Open-Share-It it is not possible to give a rating for the user or his/her foodbaskets (but parts for future release are already implemented now). Believing that our team will work together with Foodsharing one day we decided to add this feature when the website provides this function one day. The same goes for the communication channel: when we decided on the features of the application this was not supported by the website of Foodsharing. At the current time Foodsharing also has no Friendship or Following mechanism implemented. Therefore, it does not make sense to implement a feature for the mobile version if it is neither supported by the website nor by the API(= Application Programming Interface), it is still in development.

The mechanisms ’4. Present voluntarily given information to other users’ and ’5. Present voluntarily given information carefully’ are implemented in the Open-Share-It project. We have different kinds of accessing levels. For anonymous users other users are displayed by their first names and the first letter of their last names. No contact information is displayed. Logged in users see a little bit more: they can see the full name, but contact information will only be displayed if the users agree on forwarding a foodbasket.

A button to report abuse is not implemented at the current state of the project. Nevertheless, this feature should be provided in the final first version.

We give the user the possibility to control his/her data. He/she can edit his/her profile and manage his/her foodbaskets the way he/she wants.

At the current state of the project there are no explanations about used data. Therefore, the advice ’8. Explain why you need the information’ is not covered by our project. We only automatically request the user’s location to display his/her position on the map. In iOS the user has to accept this request. Otherwise, the user’s position will be displayed on the map on the last received position or if this is not possible on default coordinates. Nevertheless, information like his/her address, his/her contact information, although they seem to be self-explanatory, could be given in more detail.

The application asks for GPS data only to display them on the map. No further requests for other purposes are done. Therefore, the suggestion ’9. Avoid location-based data if not needed’ is covered.

We still try to cooperate with Foodsharing and because of that the communication from the mobile application to a server has only been partly developed. Therefore, security questions have not been handled so far.

When the application will be published, further information about security and privacy will be given. But at the current state of development it makes no sense to create privacy or security policies. With such policies and further information we also want to be as transparent as possible. Users should always know which of his/her data is displayed when, where and to whom.

The mobile application will be published as an open source project. Therefore, it fulfils the advice ’13. Use open source if it is consistent with your business objectives’. It is also a method to be more transparent. The users can always look at the source code and can make sure what is happening with their data.

We use core elements of the iOS framework for the iOS version of the mobile application to give the user a familiar and technically convincing user-interface. The application uses processes which are known from other applications. Adding a foodbasket is similar to filling a basket for a webshop. Elements, like the map, tab-bar, navigation-bar etc. are used for a familiar experience.

The guideline '16. Have features that really satisfy your users' is subjective. However, in comparison to the website, our team thinks that it has some features that can satisfy future users. We can use the GPS location system of the smartphone to locate the user's current location. The user can find his/her position easily on the map. Another interesting feature is to take pictures directly with the smartphone and to use it for items, the foodbasket or the profile image. Users can easily take pictures, which simplifies the creation process of a foodbasket.

It is easy to answer the question about advertisement: we do not use any advertisements in our project. The mechanism '18. Present feedback from users and facts' has to be considered at a later point in development.

The use of a brand would be possible if we cooperated with Foodsharing. Foodsharing already uses a brand that has a reputation and attracts media attention. This brand could create trust because users already know it from the web platform.

The last guideline '20. Do not hide log out possibilities' is a mechanism that is already implemented in the Open-Share-It mobile application. The user can easily log out whenever he/she wants to.

Guideline	Fulfilled
1. Use rating systems for users and their actions	not possible at the moment
2. Let the users communicate	not possible at the moment
3. Use following or friendship mechanism to make trust transitive	not possible at the moment
4. Present voluntarily given information to other users	yes
5. Present voluntarily given information carefully	yes
6. Let the user give you feedback	not possible at the moment
7. Let the user control his/her data	yes
8. Explain why you need the information	no
9. Avoid location-based data if not needed	yes
10. Make your application secure	not possible at the moment
11. Present your privacy and security measures	not possible at the moment
12. Be transparent	yes
13. Use open source if it is consistent with your business objectives	yes
14. Be technically convincing	yes
15. Have a good design and usability	yes
16. Have features that really satisfy your users	yes
17. Be careful with advertisements	yes
18. Present feedback from users and facts	too soon
19. Create a brand and make it public and likeable	could be possible
20. Do not hide log out possibilities	yes

Table 8.1: The table presents the results of the comparison of the guidelines with the Open-Share-It project (at the current state of development.)

8.2 Summary

In this chapter I compared the Open-Share-It project with the guidelines from the previous chapter. Many of these mechanisms are implemented or considered for the first version of the project. But there are also things that could not have been included so far. Communication between users or rating the taken foodbaskets are mechanisms that have not been possible to implement so far because they are not supported by Foodsharing at the moment.
Nevertheless, many other mechanisms are fulfilled at the moment and it will still become more for the first final version of the Open-Share-It project. For example, we already planned the project to be an open source project and we avoid requesting location data if not needed. Our project provides a good and familiar design. The user knows what is officially shown about him/her and has the opportunity to control this information. The chapter has a table in which the results are summarized.

We have already implemented a lot of these mechanisms, but there will be even more at the end of our first version. Our goal is to develop a good mobile application which satisfies the users and enhances their trust in the social network and in their users.

CHAPTER 9

Conclusion and Future Work

I used different approaches to investigate how trust can be influenced in community-based mobile applications. I developed guidelines with the help of literature research, interviews, a survey and the experiences of developing the iOS version of the Open-Share-It project. In this chapter I summarize my thesis, give a conclusion and talk about future work which could be done in this area.

9.1 Summary of the Work

In the chapter ’Introduction’ I introduced my thesis to the reader. I explained the problems, the aims and presented my methodological approaches. Finally, I told the reader how this thesis is structured. I did so to give the reader a quick overview about what he/she might expect from this thesis and cited often used companies.

In the chapter ’Basic Terms’ I explained and defined the most important terms for this thesis: trust, mobile applications and online communities. I wanted to make it clear that trust is multi-faceted and that the problem of creating trust cannot be reduced to one single solution.

The project, in which I took part and which was also influential for this paper, is described in ’Open-Share-It’. The chapter is about the different features of the mobile application, which will be implemented in the first version and which will follow further versions. Additionally, I described why the Open-Share-It project needs special attention for creating trust.

In ’Related Work’ I presented the results of my literature research. Especially in the area of e-commerce many researches about trust creation were done. I presented different approaches which can be adopted for my topic.

In the chapter ’Interviews’ I interviewed ten experts from the academic area about methods to create trust in community-based mobile applications. I presented and analyzed these results which I needed to design the guidelines.

In the chapter 'Survey' I presented the results of the questionnaire which was answered 152 times. I asked about factors that influence the user's trust in social networks, between users in such networks and in mobile applications in general. It was very informative to analyze these questionnaire. I also pointed out that men and women thought differently about some issues. The same was true for participants with some computer science education in comparison to participants without such a knowledge. It showed me once more that trust depends on many different factors.

The synthesized results were described in the chapter 'Guidelines for Trustful Mobile Applications'. I created 20 guidelines to enhance trust in community-based mobile applications. Some of them are security- or privacy-related, others are about the presentation of a mobile application. Most of them are not restricted to this topic and can be adopted for another mobile applications or even other software as well.

After defining the guidelines, I reflected these results with the Open-Share-It project in the chapter 'Comparison to the Open-Share-It Project'. I explained which of these ideas had already been integrated and which could not be considered until now. Most of them should be integrated for the final first version, but because of some problems, some of them have not been built-in yet.

9.2 Future Work

I found a lot of papers about trust in the area of e-commerce. But it was hard to get information about mobile applications - especially for community-based mobile applications. Therefore, I claim for further investigations in this area. There are a lot of unanswered questions. Answering them could help to make mobile applications better and more trustful.

For example, I found it interesting that the currently used mobile operating system has no methods to show the user that a transaction is securely transmitted in a mobile application. There are no icons or signals, as they are known from internet browsers (a green icon in the address bar, if the website is secure by using a https connection). This problem was also mentioned by the report of the Federal Trade Commission [Feda]. An icon, as we know it from iOS for the geo-location service (GPS) could, for example, be helpful if the mobile application uses an encrypted connection.

Another interesting topic, which needs further investigation, is how the use of resources from a mobile application can be transparently presented to the user. Often, the user does not know why and when his/her private information, like his/her contacts, is taken. As I explained in my thesis, further explanations can help to increase the user's trust. The Federal Trade Commission [Feda] proposes a 'privacy dashboard' in which each transaction is displayed and explained.

Further investigations could be done on how the term open source could be made more public for non-technical users and how this would effect the user's trust.

Open-Share-It is going to be a non-profit mobile application provided by some non-profit organisation. It would be interesting to know if the fact that the mobile application is for a good cause, has an influence on the user's trust.

Another interesting question would be if users see any differences in their trust relationship if they use their social network from a browser on a personal computer or from a mobile application. Or if it has an influence on their trust, when they use a HTML5 based website on their smartphone or if they use a mobile application for this purpose.

Further investigations should be carried out to find out how trust can be generated in social networks, as provided by the Open-Share-It project. Perhaps other mechanisms can be explored which can help to increase the user's trust and make the transactions of foodbaskets easier.

As one can see, there are many topics that need further investigation and I hope that my work is an inspiration for future works.

9.3 Conclusion

Trust is very important and can influence the use of a mobile application and the actions performed on it. It is multi-faceted, depends on many different things and therefore needs special attention. The absence of trust-generating mechanisms or further explanations about the taken data in mobile applications, shows that trust has less attention as it deserves.

Mobile applications and social networks are quite new technologies and need further investigation about trust in this area. At the moment, there is no icon or signal to show the user of a mobile operating system that his/her transaction is securely transmitted.
In Android a user gets informed what resources are taken by the application. But the system or the application does not tell the user when, why and how often these resources are transmitted. The use of the user's data is often not transparent and can decrease the user's trust.

The Open-Share-It project is a good example of a mobile application where trust needs special attention. The user has to trust in the social network and in other users when communicating with them. They must trust even more when meeting the other person in real life and taking the food of a mostly unknown person. The mobile application needs to support the trust creation process in every possible way. The Open-Share-It project showed how important trust creation can be. Although not each guideline could be implemented due to the fact that the first version of the application is still in development, it is important to keep this trust-relationship in mind and to take them into account for the development and further versions.

We must trust other people every day. Our actions and decisions mostly depend on our trust in someone or something. Trust is inevitable and is always present in our daily lives and should also be considered when developing software. Trust is nothing that can be produced for sure and will remain forever - trust needs special attention and has to be maintained.

So, let the users get a great experience, satisfy them - let them trust in you and your application.

APPENDIX A

Appendix

A.1 Figures

Screenshots from Open-Share-It

In the following further screenshots of the Open-Share-It project are presented.

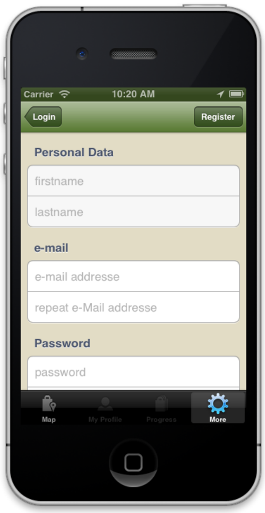


Figure A.1: Register view in the Open-Share-It application.

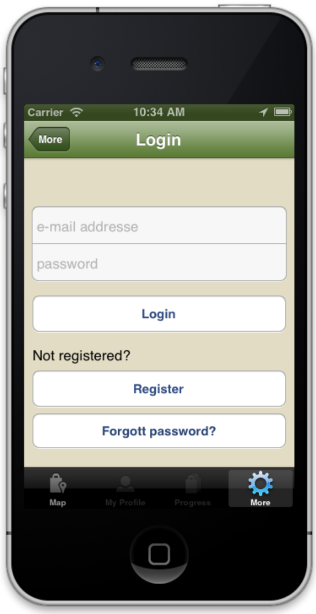


Figure A.2: Login view in the Open-Share-It application.

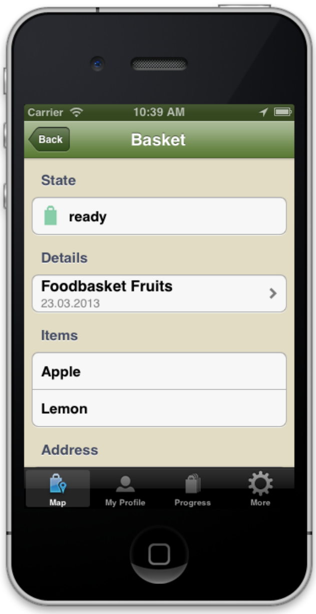
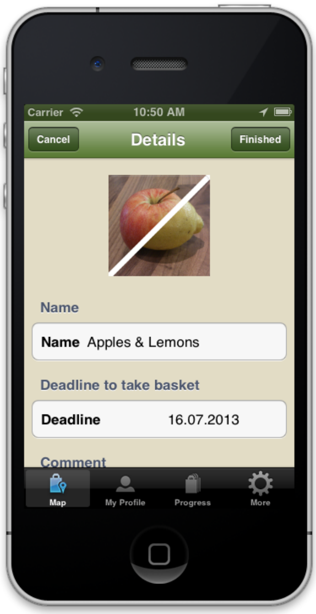


Figure A.3: Presentation of a foodbasket in the Open-Share-It application.



Name

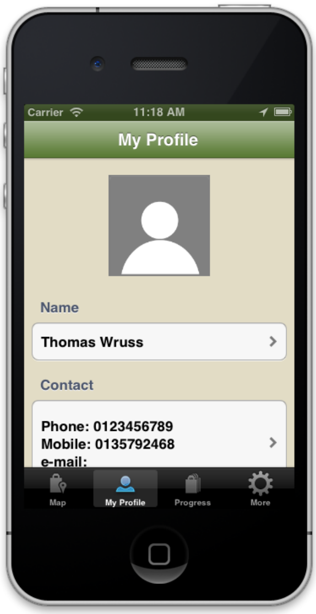
Name Apples & Lemons

Deadline to take basket

Deadline 16.07.2013

Comment

Figure A.4: Details view of a foodbasket in the Open-Share-It application.



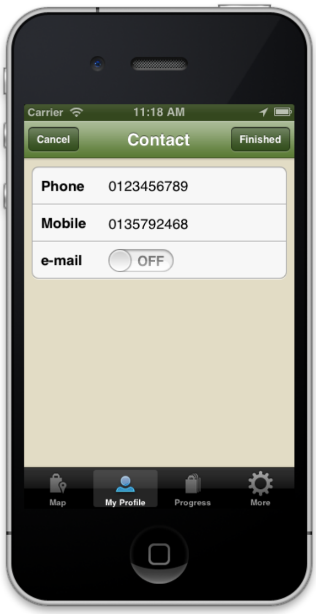
Name

Thomas Wruss

Contact

Phone: 0123456789
Mobile: 0135792468
e-mail:

Figure A.5: Profile view in the Open-Share-It application.

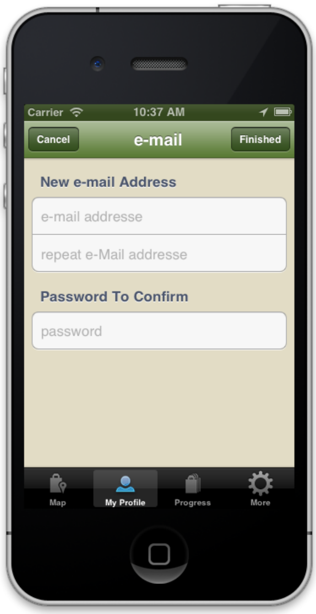


Phone 0123456789

Mobile 0135792468

e-mail OFF

Figure A.6: Contact view of the own profile in the Open-Share-It application.



New e-mail Address

e-mail addresse

repeat e-Mail addresse

Password To Confirm

password

Figure A.7: View for editing e-mail address of the own profile in the Open-Share-It application.

Charts from the results of the questionnaire

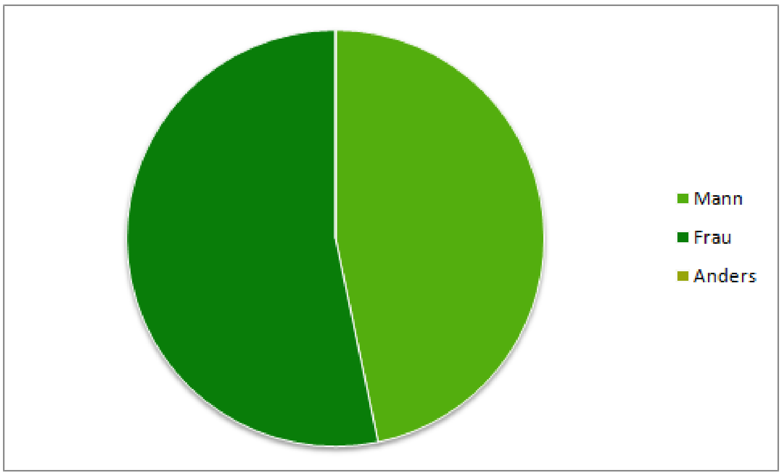


Figure A.8: Questionnaire distribution by sex.

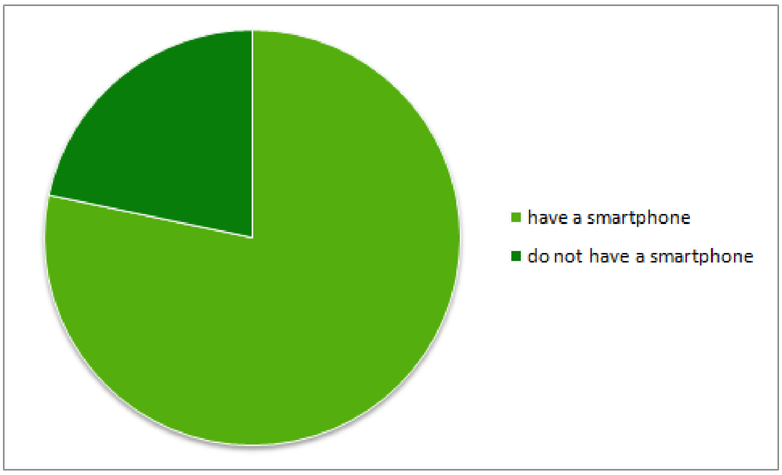
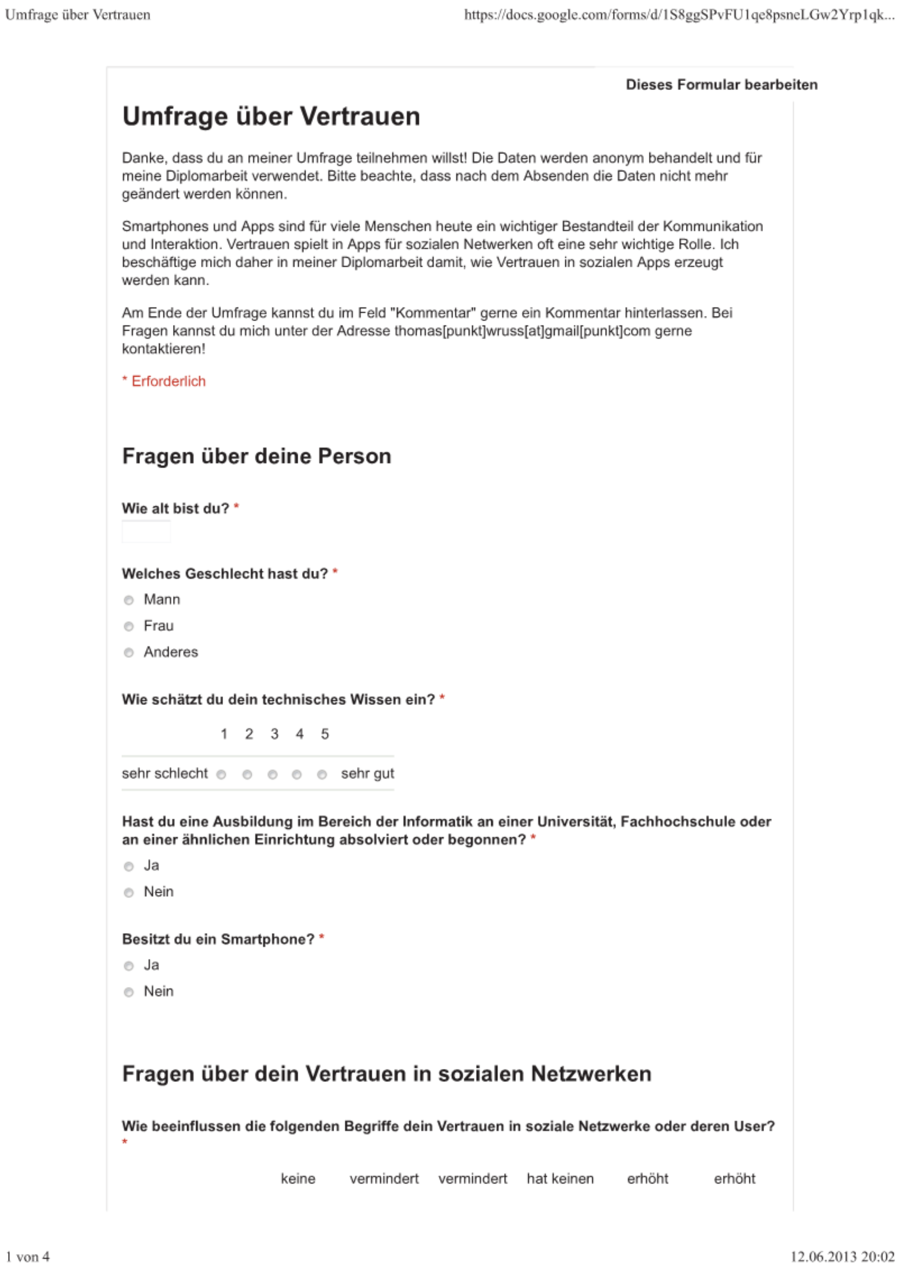


Figure A.9: Questionnaire distribution by smartphones.

A.2 Questionnaire

In this section screenshots from the online-questionnaire are presented.



Umfrage über Vertrauen https://docs.google.com/forms/d/1S8ggSPvFU1qe8psneLGw2Yrp1qk...

Dieses Formular bearbeiten

Umfrage über Vertrauen

Danke, dass du an meiner Umfrage teilnehmen willst! Die Daten werden anonym behandelt und für meine Diplomarbeit verwendet. Bitte beachte, dass nach dem Absenden die Daten nicht mehr geändert werden können.

Smartphones und Apps sind für viele Menschen heute ein wichtiger Bestandteil der Kommunikation und Interaktion. Vertrauen spielt in Apps für sozialen Netwerken oft eine sehr wichtige Rolle. Ich beschäftige mich daher in meiner Diplomarbeit damit, wie Vertrauen in sozialen Apps erzeugt werden kann.

Am Ende der Umfrage kannst du im Feld "Kommentar" gerne ein Kommentar hinterlassen. Bei Fragen kannst du mich unter der Adresse thomas[punkt]wruss[at]gmail[punkt]com gerne kontaktieren!

* Erforderlich

Fragen über deine Person

Wie alt bist du? *

Welches Geschlecht hast du? *

○ Mann

○ Frau

○ Anderes

Wie schätzt du dein technisches Wissen ein? *

	1	2	3	4	5	
sehr schlecht	○	○	○	○	○	sehr gut

Hast du eine Ausbildung im Bereich der Informatik an einer Universität, Fachhochschule oder an einer ähnlichen Einrichtung absolviert oder begonnen? *

○ Ja

○ Nein

Besitzt du ein Smartphone? *

○ Ja

○ Nein

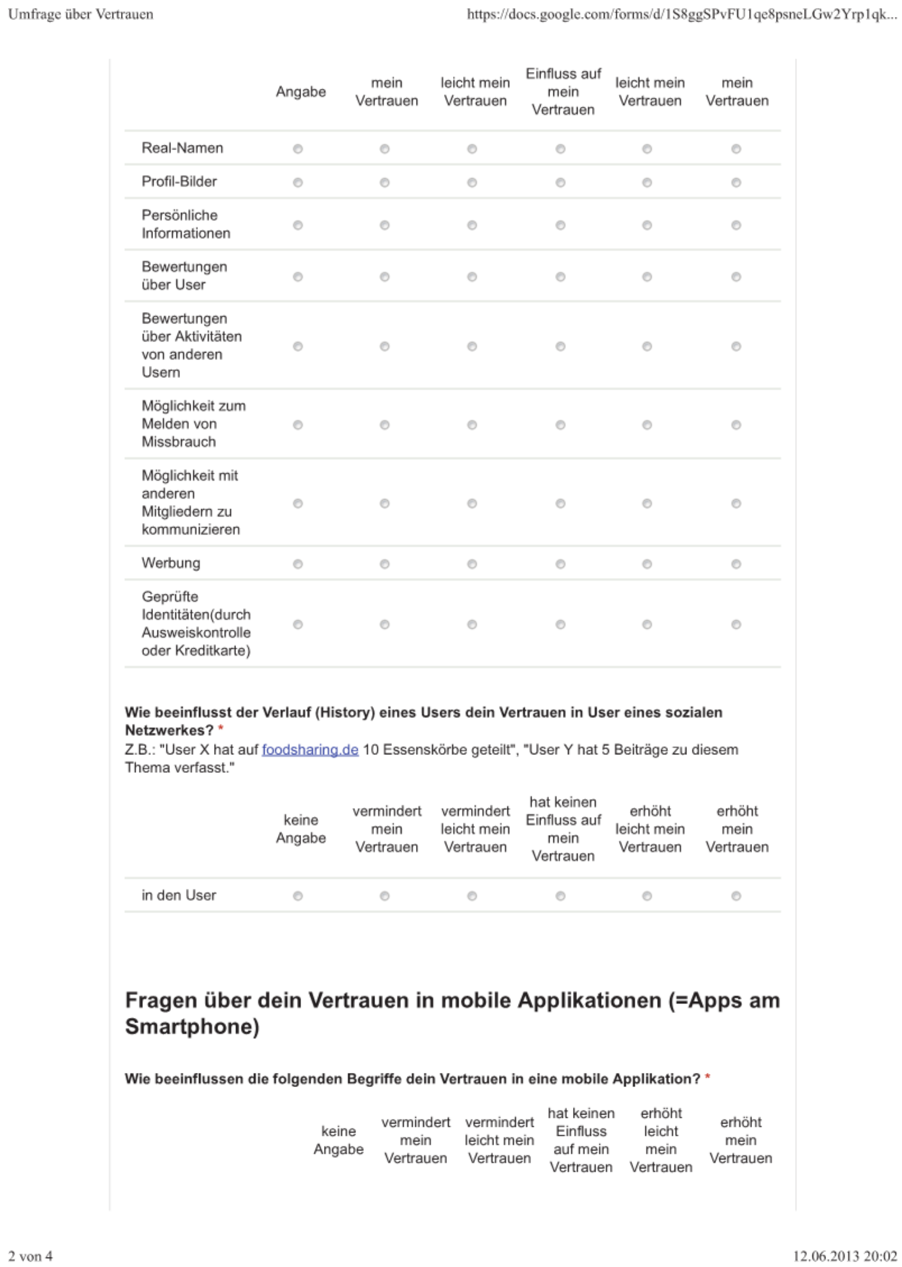
Fragen über dein Vertrauen in sozialen Netzwerken

Wie beeinflussen die folgenden Begriffe dein Vertrauen in soziale Netzwerke oder deren User? *

	keine	vermindert	vermindert	hat keinen	erhöht	erhöht

1 von 4 12.06.2013 20:02

Figure A.10: Page 1 of the questionnaire.



Umfrage über Vertrauen https://docs.google.com/forms/d/1S8ggSPvFU1qe8psneLGw2Yrp1qk...

	Angabe	mein Vertrauen	leicht mein Vertrauen	Einfluss auf mein Vertrauen	leicht mein Vertrauen	mein Vertrauen
Real-Namen	○	○	○	○	○	○
Profil-Bilder	○	○	○	○	○	○
Persönliche Informationen	○	○	○	○	○	○
Bewertungen über User	○	○	○	○	○	○
Bewertungen über Aktivitäten von anderen Usern	○	○	○	○	○	○
Möglichkeit zum Melden von Missbrauch	○	○	○	○	○	○
Möglichkeit mit anderen Mitgliedern zu kommunizieren	○	○	○	○	○	○
Werbung	○	○	○	○	○	○
Geprüfte Identitäten(durch Ausweiskontrolle oder Kreditkarte)	○	○	○	○	○	○

Wie beeinflusst der Verlauf (History) eines Users dein Vertrauen in User eines sozialen Netzwerkes? *
Z.B.: "User X hat auf foodsharing.de 10 Essenskörbe geteilt", "User Y hat 5 Beiträge zu diesem Thema verfasst."

	keine Angabe	vermindert mein Vertrauen	vermindert leicht mein Vertrauen	hat keinen Einfluss auf mein Vertrauen	erhöht leicht mein Vertrauen	erhöht mein Vertrauen
in den User	○	○	○	○	○	○

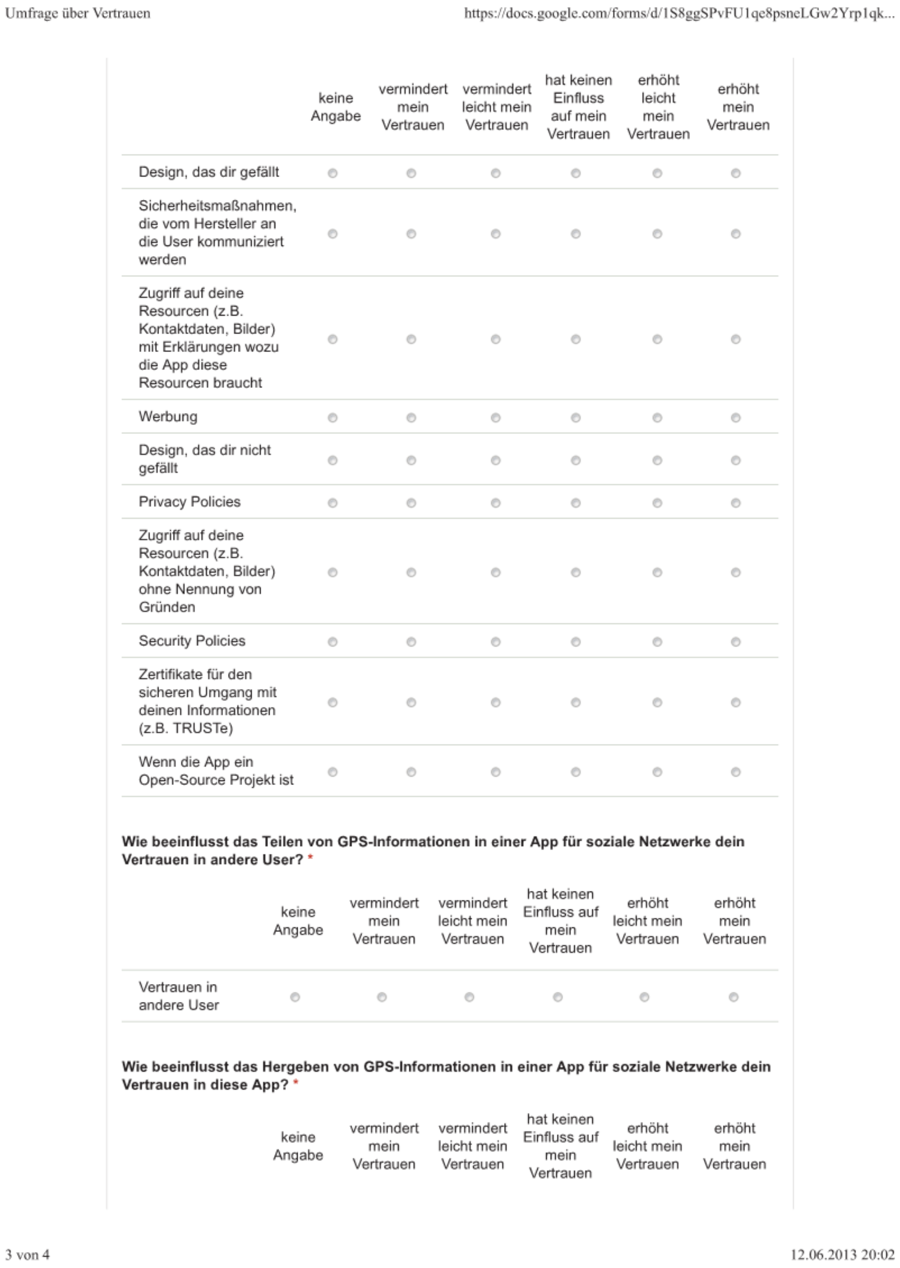
Fragen über dein Vertrauen in mobile Applikationen (=Apps am Smartphone)

Wie beeinflussen die folgenden Begriffe dein Vertrauen in eine mobile Applikation? *

	keine Angabe	vermindert mein Vertrauen	vermindert leicht mein Vertrauen	hat keinen Einfluss auf mein Vertrauen	erhöht leicht mein Vertrauen	erhöht mein Vertrauen

2 von 4 12.06.2013 20:02

Figure A.11: Page 2 of the questionnaire.



Umfrage über Vertrauen https://docs.google.com/forms/d/1S8ggSPvFU1qe8psneLGw2Yrp1qk...

	keine Angabe	vermindert mein Vertrauen	vermindert leicht mein Vertrauen	hat keinen Einfluss auf mein Vertrauen	erhöht leicht mein Vertrauen	erhöht mein Vertrauen
Design, das dir gefällt	○	○	○	○	○	○
Sicherheitsmaßnahmen, die vom Hersteller an die User kommuniziert werden	○	○	○	○	○	○
Zugriff auf deine Resourcen (z.B. Kontaktdaten, Bilder) mit Erklärungen wozu die App diese Resourcen braucht	○	○	○	○	○	○
Werbung	○	○	○	○	○	○
Design, das dir nicht gefällt	○	○	○	○	○	○
Privacy Policies	○	○	○	○	○	○
Zugriff auf deine Resourcen (z.B. Kontaktdaten, Bilder) ohne Nennung von Gründen	○	○	○	○	○	○
Security Policies	○	○	○	○	○	○
Zertifikate für den sicheren Umgang mit deinen Informationen (z.B. TRUSTe)	○	○	○	○	○	○
Wenn die App ein Open-Source Projekt ist	○	○	○	○	○	○

Wie beeinflusst das Teilen von GPS-Informationen in einer App für soziale Netzwerke dein Vertrauen in andere User? *

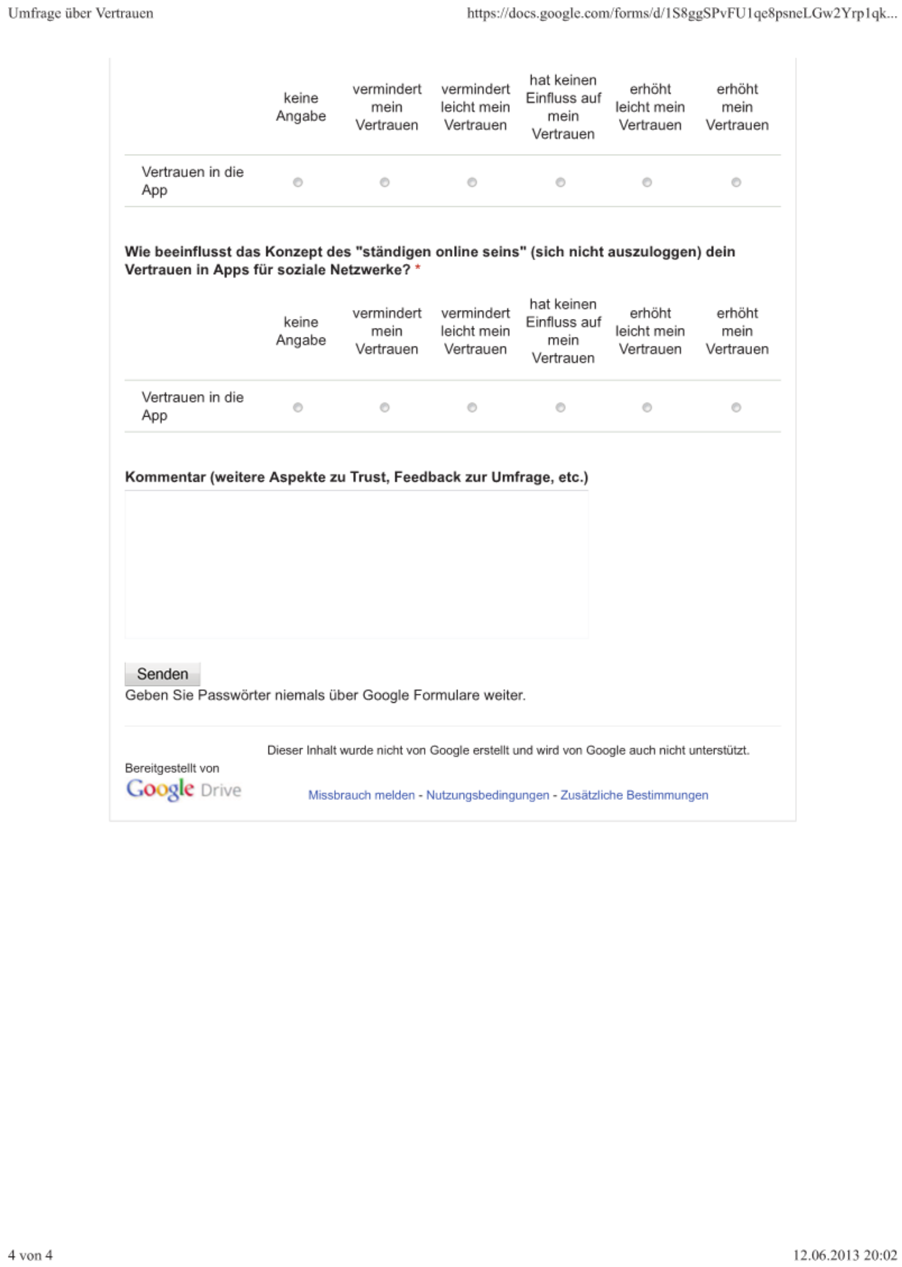
	keine Angabe	vermindert mein Vertrauen	vermindert leicht mein Vertrauen	hat keinen Einfluss auf mein Vertrauen	erhöht leicht mein Vertrauen	erhöht mein Vertrauen
Vertrauen in andere User	○	○	○	○	○	○

Wie beeinflusst das Hergeben von GPS-Informationen in einer App für soziale Netzwerke dein Vertrauen in diese App? *

	keine Angabe	vermindert mein Vertrauen	vermindert leicht mein Vertrauen	hat keinen Einfluss auf mein Vertrauen	erhöht leicht mein Vertrauen	erhöht mein Vertrauen

3 von 4 12.06.2013 20:02

Figure A.12: Page 3 of the questionnaire.



Umfrage über Vertrauen https://docs.google.com/forms/d/1S8ggSPvFU1qe8psneLGw2Yrp1qk...

	keine Angabe	vermindert mein Vertrauen	vermindert leicht mein Vertrauen	hat keinen Einfluss auf mein Vertrauen	erhöht leicht mein Vertrauen	erhöht mein Vertrauen
Vertrauen in die App	○	○	○	○	○	○

Wie beeinflusst das Konzept des "ständigen online seins" (sich nicht auszuloggen) dein Vertrauen in Apps für soziale Netzwerke? *

	keine Angabe	vermindert mein Vertrauen	vermindert leicht mein Vertrauen	hat keinen Einfluss auf mein Vertrauen	erhöht leicht mein Vertrauen	erhöht mein Vertrauen
Vertrauen in die App	○	○	○	○	○	○

Kommentar (weitere Aspekte zu Trust, Feedback zur Umfrage, etc.)

Geben Sie Passwörter niemals über Google Formulare weiter.

Dieser Inhalt wurde nicht von Google erstellt und wird von Google auch nicht unterstützt.

Bereitgestellt von Google Drive

Missbrauch melden - Nutzungsbedingungen - Zusätzliche Bestimmungen

4 von 4 12.06.2013 20:02

Figure A.13: Page 4 of the questionnaire.

Bibliography

[AA03] I. Araujo and I. Araujo. Developing trust in internet commerce. In *Proceedings of the 2003 conference of the Centre for Advanced Studies on Collaborative research*, CASCON '03, pages 1–15, 2003.

[AEG$^+$10] S. Adali, R. Escriva, M. Goldberg, M. Hayvanovych, M. Magdon-Ismail, B. Szymanski, W. Wallace, and G. Williams. Measuring behavioral trust in social networks. In *Intelligence and Security Informatics (ISI), 2010 IEEE International Conference on*, pages 150–152, 2010.

[APC10] Z. M. Aljazzaf, M. Perry, and M. A. M. Capretz. Online trust: Definition and principles. In *Computing in the Global Information Technology (ICCGI), 2010 Fifth International Multi-Conference on*, pages 163–168, 2010.

[ARH00] A. Abdul-Rahman and S. Hailes. Supporting trust in virtual communities. In *System Sciences, 2000. Proceedings of the 33rd Annual Hawaii International Conference on*, pages 9 pp. vol.1–, 2000.

[Bar83] B. Barber. *The logic and limits of trust.* Rutgers University Press, 1983.

[BBJ11] N. Bosilj, G. Bubas, and M. Jadric. The influence of users' attitudes regarding trust, privacy and control on the adoption of mobile advertising. In *MIPRO, 2011 Proceedings of the 34th International Convention*, pages 1420–1425, 2011.

[BBK94] T. Beth, M. Borcherding, and B. Klein. Valuation of trust in open networks. In *Computer Security — ESORICS 94*, volume 875 of *Lecture Notes in Computer Science*, pages 1–18. 1994.

[BBRS06] R. Ballagas, J. Borchers, M. Rohs, and J. Sheridan. The smart phone: a ubiquitous input device. *Pervasive Computing, IEEE*, 5(1):70–77, 2006.

[Ber00] H. Bernard. *Social research methods: qualitative and quantitative approaches.* SAGE Publications, Incorporated, 2000.

[BS02] S. Braynov and T. Sandholm. Contracting with uncertain level of trust. *Computational Intelligence*, 18(4):501–514, 2002.

[CFSW12] E. Chin, A. P. Felt, V. Sekar, and D. Wagner. Measuring user confidence in smartphone security and privacy. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, SOUPS '12, pages 1:1–1:16, 2012.

[FA11] M. Faisal and A. Alsumait. Social network privacy and trust concerns. In *Proceedings of the 13th International Conference on Information Integration and Web-based Applications and Services*, iiWAS '11, pages 416–419, 2011.

[FAMA12] S. Fusco, R. Abbas, K. Michael, and A. Aloudat. Location-based social networking: Impact on trust in relationships. *Technology and Society Magazine, IEEE*, 31(2):39–50, 2012.

[Feda] Federal Trade Commission. Mobile privacy disclosures, building trust through transparency. Retrieved May 27, 2013, from `http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf`.

[Fedb] Federal Trade Commission. Protecting consumer privacy in an era of rapid change. Retrieved July 24, 2013, from `http://ftc.gov/os/2012/03/120326privacyreport.pdf`.

[Fer98] A. Ferraro. Electronic commerce: The issues and challenges to creating trust and a positive image in consumer sales on the world wide web. *First Monday*, 3(6), 1998.

[Fin03a] A. Fink. *The Survey Handbook*. The Survey Kit. SAGE Publications, 2003.

[Fin03b] A. Fink. *The Survey Kit: How to ask survey questions*. The Survey Kit. SAGE Publications, 2003.

[FKH00] B. Friedman, P. H. Khan, Jr., and D. C. Howe. Trust online. *Commun. ACM*, 43(12):34–40, 2000.

[Gam90] D. Gambetta. Can We Trust Trust? In *Trust: Making and Breaking Cooperative Relations*, pages 213–237, 1990.

[Gef00] D. Gefen. E-commerce: the role of familiarity and trust. *Omega*, 28(6):725–737, 2000.

[GH02] J. Gubrium and J. Holstein. *Handbook of Interview Research: Context and Method*. A SAGE reference title. SAGE Publications, 2002.

[GS00] T. Grandison and M. Sloman. A survey of trust in internet applications. *Communications Surveys Tutorials, IEEE*, 3(4):2–16, 2000.

[Hsu08] C.-J. Hsu. Dominant factors for online trust. In *Cyberworlds, 2008 International Conference on*, pages 165–172, 2008.

[JGS82] C. Johnson-George and W. C. Swap. Measurement of specific interpersonal trust: Construction and validation of a scale to assess trust in a specific other. *Journal of Personality and Social Psychology*, 43(6):1306–1317, 1982.

[Joh] R. Johnson. Scaling facebook to 500 million users and beyond. Retrieved April 22, 2013, from https://www.facebook.com/note.php?note_id=409881258919&id=9445547199&ref=mf.

[Jøs96] A. Jøsang. The right type of trust for distributed systems. In *Proceedings of the 1996 workshop on New security paradigms*, pages 119–131, 1996.

[Koe03] D. Koehn. The nature of and conditions for online trust. *Journal of Business Ethics*, 43(1-2):3–19, 2003.

[Kor] A. Korff. Tips for building trust with your clients. Retrieved June 20, 2013, from http://sixrevisions.com/project-management/tips-build-trust-clients/.

[Kos10] T. Kosa. Vampire bats: Trust in privacy. In *Privacy Security and Trust (PST), 2010 Eighth Annual International Conference on*, pages 96–102, 2010.

[LFH10] J. Lazar, J. Feng, and H. Hochheiser. *Research Methods in Human-Computer Interaction*. John Wiley & Sons, 2010.

[LH04] P. Lanford and R. Hübscher. Trustworthiness in e-commerce. In *Proceedings of the 42nd annual Southeast regional conference*, ACM-SE 42, pages 315–319, 2004.

[LY09] F. Lin and W. Ye. Operating system battle in the ecosystem of smartphone industry. In *Information Engineering and Electronic Commerce, 2009. IEEC '09. International Symposium on*, pages 617–621, 2009.

[MDS95] R. C. Mayer, J. H. Davis, and F. D. Schoorman. An integrative model of organizational trust. *The Academy of Management Review*, 20(3):pp. 709–734, 1995.

[MNHZ10] D. Moreland, S. Nepal, H. Hwang, and J. Zic. A snapshot of trusted personal devices applicable to transaction processing. *Personal Ubiquitous Comput.*, 14(4):347–361, 2010.

[Nis99] H. Nissenbaum. Can trust be secured online? a theoretical perspective. *Etica & Politica*, 2, 1999.

[Pal] C. Palihapitiya. Facebook mobile: 100 million and growing. Retrieved April 22, 2013, from http://www.facebook.com/blog/blog.php?post=297879717130.

[PCFJ03] T. Punter, M. Ciolkowski, B. Freimut, and I. John. Conducting on-line surveys in software engineering. In *Empirical Software Engineering, 2003. ISESE 2003. Proceedings. 2003 International Symposium on*, pages 80–88, 2003.

[Pet] B. Petersen. Social platforms gwi.8 update: Decline of local social media platforms. Retrieved May 12, 2013, from http://www.globalwebindex.net/social-platforms-gwi-8-update-decline-of-local-social-media-platforms/.

[Rei97] G. L. Rein. Definition of community. *SIGGROUP Bull.*, 18(1):43–44, 1997.

[RSBC98] D. M. Rousseau, S. B. Sitkin, R. S. Burt, and C. Camerer. Not so different after all: A cross-discipline view of trust. *Academy of management review*, 23(3):393–404, 1998.

[Shn00] B. Shneiderman. Designing trust into online experiences. *Commun. ACM*, 43(12):57–59, 2000.

[SKY07] R. Song, L. Korba, and G. Yee. *Trust in E-Services: Technologies, Practices, and Challenges*. Igi Global, 2007.

[SLD11] S. Sousa, D. Lamas, and P. Dias. The interrelation between communities, trust and their online social patterns. In *Dependable, Autonomic and Secure Computing (DASC), 2011 IEEE Ninth International Conference on*, pages 980–986, 2011.

[SS03] K. Siau and Z. Shen. Building customer trust in mobile commerce. *Commun. ACM*, 46(4):91–94, 2003.

[Sta07] W. Stallings. *Data And Computer Communications, 8/E*. Pearson Education, 2007.

[Ste04] S. Steinbrecher. Balancing privacy and trust in electronic marketplaces. In *Trust and Privacy in Digital Business*, volume 3184 of *Lecture Notes in Computer Science*, pages 70–79. 2004.

[SY00] D. Schoder and P.-L. Yin. Building firm trust online. *Commun. ACM*, 43(12):73–79, 2000.

[TF99] S. Tseng and B. J. Fogg. Credibility and computing technology. *Commun. ACM*, 42(5):39–44, 1999.

[Uli05] F. Ulivieri. Social approaches to trust-building in web technologies. In *Security and Privacy for Emerging Areas in Communication Networks, 2005. Workshop of the 1st International Conference on*, pages 51–60, 2005.

[weba] Android and iOS Combine for 91.1% of the Worldwide Smartphone OS Market in 4Q12 and 87.6% for the Year, According to IDC . Retrieved April 23, 2013, from `http://www.idc.com/getdoc.jsp?containerId=prUS23946013`.

[webb] Facebook reports first quarter 2013 results. Retrieved May 12, 2013, from `http://investor.fb.com/releasedetail.cfm?ReleaseID=761090`.

[webc] PC Shipments Expected to Have Strong Second Half of 2012, Long-Term PC Growth Capped Within Single Digits, According to IDC. Retrieved April 23, 2013, from `http://www.idc.com/getdoc.jsp?containerId=prUS23371512`.

[webd] Smartphone, tablet sales outpace pc growth. Retrieved April 23, 2013, from http://graphics.thomsonreuters.com/12/02/GLB_TECHMKTB0212_SC.html.

[Wei08] R. Weiss. *Learning From Strangers: The Art and Method of Qualitative Interview Studies*. Free Press, 2008.

[WJB08] Z. Weiguo, L. Jun, and W. Bingshan. Study on the trust mechanism in communities of practice. In *Automation and Logistics, 2008. ICAL 2008. IEEE International Conference on*, pages 2116–2119, 2008.

[WLZS11] L. Wang, F. Liu, Y. Zhao, and K. Shi. Exploring the influencing factors on surfing behavior intention of smartphone users. In *Advanced Computational Intelligence (IWACI), 2011 Fourth International Workshop on*, pages 688–692, 2011.

[Yal11] R. Yale. Welcome to i-berspace: Media gratifications in successful virtual communities. *Virtual sociability: From community to communitas*, pages 101–118, 2011.

[YPF$^+$05] S. Y. Yousafzai, J. Pallister, G. R. Foxall, et al. Strategies for building and communicating trust in electronic banking: A field experiment. *Psychology & Marketing*, 22(2):181–201, 2005.

[ZJ12] G. Zhang and E. K. Jacob. Community: issues, definitions, and operationalization on the web. In *Proceedings of the 21st international conference companion on World Wide Web*, WWW '12 Companion, pages 1121–1130, 2012.