Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

Report

Proceedings of the User-Centered Trust in Interactive Systems Workshop: a Workshop from NordiCHI 2012

Report no 1028
Editor Trenton Schulz

Date March 22, 2013
ISBN 978-82-539-0538-9

Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

The editor

Trenton Schulz is a research scientist at Norsk Regnesentral and is part of the e-inclusion group. Trenton leads Norsk Regnesentral's work in the EU project uTRUSTit, which involves, among other things, looking at accessibility of the Internet of Things. He has several years of experience in software development, working on both libraries, desktop, and mobile applications.

Norwegian Computing Center

Norsk Regnesentral (Norwegian Computing Center, NR) is a private, independent, non-profit foundation established in 1952. NR carries out contract research and development projects in the areas of information and communication technology and applied statistical modeling. The clients are a broad range of industrial, commercial and public service organizations in the national as well as the international market. Our scientific and technical capabilities are further developed in co-operation with The Research Council of Norway and key customers. The results of our projects may take the form of reports, software, prototypes, and short courses. A proof of the confidence and appreciation our clients have for us is given by the fact that most of our new contracts are signed with previous customers.

Norsk Regnesentral
Norwegian Computing Center
Postboks 114, Blindern
NO-0314 Oslo, Norway

Besøksadresse
Office address
Gaustadalléen 23
NO-0373 Oslo, Norway

Telefon · telephone
(+47) 22 85 25 00
Telefaks · telefax
(+47) 22 69 76 60

Internett · internet
www.nr.no
E-post · e-mail
nr@nr.no

Title	**Proceedings of the User-Centered Trust in Interactive Systems Workshop: a Workshop from NordiCHI 2012**
Editor	**Trenton Schulz** <trenton.schulz@nr.no>
Date	March 22, 2013
ISBN	978-82-539-0538-9
Publication number	1028
Contributers	Cédric Bach, Elke Beck, Josep Blat, Marc Busch, Ralph Bruder, Maël Cornil, Caio Stein D'Agostini, Susen Döbelt, Lothar Fritsch, Laura Gheorghe, Basil Hess, Christina Hochleitner, Michaela Kauer, Ioannis Kounelis, Jan Loeschner, Benoît Otjacques, Thomas Pfeiffer, Felix von Reischach, Valeria Righi, Andrea Rosales, Till Halbach Røssvoll, Sergio Sayago, Mickaël Stefas, Sandra Trösterer, Manfred Tscheligi, Marco Winckler

Abstract

This report includes proceedings of the papers that were presented at the User-Centered Trust in Interactive Systems Workshop. This workshop was held on 14 October 2012 in Copenhagen as part of ACM's NordiCHI conference. It was organized by both the uTRUSTit and the Aniketos project. There are eight papers that cover issues like definitions of trust in interactive systems, factors that contribute to trust, and methods to measure trust.

Keywords	uTRUSTit, Anekitos, trust, trust factors, trust measurements, user-centered design
Target group	Everyone
Availability	Open
Project	uTRUSTit
Project number	Grant agreement no: 258360
Research field	Trustworthy ICT
Number of pages	61

Contents

1 Introduction

This is a collection of the papers that were presented at the User-Centered Trust in Interactive Systems Workshop. This workshop was part of the Seventh NordiCHI conference that was held in Copenhagen, Denmark. The workshop was a joint effort between two EU projects: Aniketos and uTRUSTit. The organizers for the workshop were CURE—Center for Usability Research and Engineering in Vienna, Austria; ICT&S Center of the University of Salzburg (Austria); and the Norwegian Computing Center in Oslo, Norway.

About the Workshop

Trust is increasingly important in several information communication technology (ICT) related areas. Nevertheless, there is still no unified definition of trust in technologies.

This full day workshop brought together researchers, experts, and practitioners to discuss and create a more unified understanding and definition of trust, as well as related research areas and methods, as a basis for a working community.

Motivation

Human trust in technologies is increasingly important, as the number of applications using confidential data of the user is steadily rising. Websites require users to enter credit card information; intelligent homes support the residents based on their behavior; and location-based services on mobile devices are frequently used in our daily lives. As technologies pervade our lives and they become more complex, it is crucial to inform users about security and privacy issues and create justified trust in ICT systems.

Yet, there is no common understanding of how a user's trust in a certain technology can be defined and what factors evoke and support trust. According to Wang and Emurian[1], two main reasons for multiple definitions of trust can be identified:

1. Trust is an abstract concept and is often used interchangeably with related concepts such as credibility, reliability, or confidence.
2. Trust is a multi-faceted, subjective concept that incorporates cognitive, emotional, and behavioral dimensions.

To investigate trust in interactive technologies and to design trustworthy applications, we need to share a common understanding of trust. So far, the trust issue has been discussed in the HCI community very broadly within workshops at CHI, CSCW, or SOUPS with respect to usable privacy, security, risk, and online trust, thereby considering different objects of trust (e.g., websites, companies, individuals). Furthermore, trust has been

1. Wang, Y. and Emurian, H. An overview of online trust: Concepts, elements, and implications, 2005

discussed generally as a factor within user experience workshops (e.g., at NordiCHI 06).

Topics

The papers presented at the workshop and included in these proceedings are based on the following topics:

- Definitions of trust in interactive systems: which definitions do exist and are incorporated in research?
- Contributing factors to trust, such as e.g. reliability, benevolence, vulnerability: which factors have to be considered about the trustor and the trustee?
- Methods to measure trust, such as e.g. questionnaires, physiological measures, behavioral observation

Activities at the Workshop

The workshop began with an introduction of the Aniketos and uTRUSTit projects. Afterwards, there was a short presentation about the problems with defining trust. Then, each of the papers was presented by one of the authors with opportunities for questions. In total, there were eight papers presented and twelve attendees at the workshop.

The afternoon session began with each participant presenting a piece of software or hardware and explained why the participant trusted it. There were many different objects that were presented. Some of the objects were mobile phones, smartphone apps, and mundane objects like a pen and paper.

Next, we created three stations for each of the workshop topics: definition of trust, contributing factors to trust, and methods to measure trust. Participants were then divided up into groups and assigned a station. One person was a recorder. The recorder stayed at a station and wrote down the different ideas from group members. After twenty minutes, the groups would rotate to another station. The recorder would then inform the new group at the station what had been discussed before and the new group would add more information for the next twenty minutes. This continued until all groups had a chance to participate at each station. Once all the groups were finished, the results were presented to the entire workshop. Figure 1.1 shows a presentation of the results the discussion groups near the end of the workshop. A quick summary of the results is presented below.

Definition of Trust in Interactive Systems

Finding a trust definition brought up many different topics. One topic was to look at the definition that was presented at the beginning of the workshop and look at the idea of *expectation of behavior*. This lead to a discussion of risk: being willing to open oneself up for risk, how one can perceive risk, and also realizing that there is always some sort of risk in most activities. The expectation of behavior also includes the idea of past experience and the idea of verifying what an object has done in the past. This is summarized in an old German saying, "trust is good; verification is better."

Figure 1.1. Presentation of results from group discussions.

There was also a real discussion about what trust means when talking about a thing. A portable gaming system was used as an example. Here, the thing that needs to be trusted is the hardware, the battery, and the software. Yet, if the device is network capable, there may be other things that need to be trusted. Another discussion focused on the idea of centralized trust (the certificate system) or decentralized trust (a web of trust).

Another suggestion was to look at trust in the same way as the OSI networking model. The reasoning here was that trust was built upon multiple levels and trust must travel up and down these levels when interacting with the trustor and the trustee, just like networks. The suggestion was to put the person or legal entitiy at level eight (the top level).

One of the groups took a look at some of the literature that had been mentioned during the opening presentations. This included O'Hara's work [2] that created a function for trust with different inputs. This lead to discussion over the inputs. Specifically, the context input contains lots of different information such as, time, previous experience, and benefits. In the end, however, we could not settle on a good definition of trust in interactive systems, but we felt that we had maybe gotten a step further.

2. http://eprints.soton.ac.uk/341800/

Contributing Factors to Trust

This began with a general discussion on the difference between factors and attributes. Attributes can be considered values or characteristics of a certain factor. Influencing factors can be split up into four different areas:

- context,
- trustor (the person trusting),
- interaction, and
- trustee (the object or person being trusted)

When looking at context, factors that could influence trust include how risky a situation is—trust may be lower in situations that have more risk. Social pressure might be another factor. After all, if everyone else is trusting the object, why shouldn't you? Emergency situations can also affect trust. The trustor probably has very little choice other than trusting in these situations. Finally, if a trustor has spent more time with a system, the trustor may be willing to take a larger risk.

The groups were able to identify several factors for the trustor. This included the trustor's mental model and how much this stystem matched that model. How the trustor perceived the system's trust-related features. How much control the trustor has over the system. Different impairments of the trustor (for example, cognitive, vision, or hearing). The background knowledge on security and privacy, experience, and skills were also named as possible factors affecting the trustor.

Less things were discussed about factors for interaction, but the idea that elaborate interactions for users and and previous interactions could be factors affecting trust.

Finally, there were many factors affecting trust of the trustee (the actual object being used by the trustor). This included information about the trustee, its security and privacy, feedback from the system, transparency to how it works, how simple it is to use, if it was possible to verify what it said it was doing, the price of the object, and its design. Another factor discussed was the trustee's reputation or its public image based on evaluations, manuafacturer, or reviews. There was also discussion about predictability versus an adaptive system. Some felt that an adaptive system might decrease perdictability, but it might make people feel better if they knew the system adapted its security.

Methods to Measure Trust

The first group discussion was focused on the different layers of trust measurement. First ideas of trust measurement were focused on behavioral indicators. Suggestions for measurements were:

- Asking
- Observing actions; e.g. risky behavior, click behavior, reaction times
- Eye tracking

The participants stated that trustworthiness is not measureable because it is a subjective impression.

The initial statement of the second group discussion was: when it comes to trust measurement, one should differentiate between methodology and metrics. The central aim is to measure a special (trust indicating) way of interaction. Potential variables of trust measurement are first based on the methods of interaction (input possibilities) e.g., gestures or mouse. Furthermore, if we assume that trust is a multilayered concept—emotional, cognitive and behavioral—there should be a multilayered measurement concept for the assessment of trust. Regarding behavioral indicators, the group discussion concluded that it is binary in it's nature in contrast to the other layers. Therefore a unique identifier for a trust indicating behavior is necessary. The participants decided that a unique trust interaction is hard to define.

The participants of the third group discussion argued if trust was measurable or just the trustworthiness of a system. Something that was in opposition to the earlier group. The discussion lead to two suggestions for measurement:

- Willingness to behave in a trust indicating way
- Analysis of exploration behavior

Conclusion

After these discussions, the idea was to attempt to build a group on the Mendeley platform and LinkedIn for further discussion of trust research. This group can be found on Mendeley's website[3] and LinkedIn[4]. Others are encouraged to join! We also decided to create this book of proceedings that we have today. The results from the work here were folded into a final version of the trust whitepaper for the uTRUSTit project[5].

3. http://www.mendeley.com/groups/2690631/user-centered-trust-in-interactive-systems/
4. http://www.linkedin.com/groups?home=&gid=4674078&trk=anet_ug_hm&goback=%2Egmp_4674078
5. Döbelt, S., Busch, M., and Hochleitner, C. Defining, Understanding, Explaining TRUST within the uTRUSTit Project. Vienna, Austria, 2012.

2 About uTRUSTit

uTRUSTit—Usable Trust in the Internet of Things—is an international collaboration between six organizations from six various countries aiming at integrating the user directly in the trust chain, guaranteeing transparency in the underlying security and reliablilty properties of the Internet of Things. The project is supported by the EU under Framework Programme 7.

The Internet of Things (IoT) will connect a large number of communication and information systems. These systems will be part of everyday life in the same way mobile phones have become part of our lives. The information security properties of the IoT are often difficult to understand for its users, because they are hidden in pervasive systems and small devices manufactured by a large number of vendors. Trustworthiness, security functions and privacy implications are vast, and must be assessable to users and consumers.

The results of uTRUSTit enable system manufacturers and system integrators to express the underlying security concepts to users in a comprehensible way, allowing them to make valid judgements on the trustworthiness of such systems. Further, uTRUSTit's design guidelines on trust help the industry to implement the trust-feedback toolkit developed by uTRUSTit in a secure, usable and accessible way.

3 About Aniketos

Aniketos (Greek for "never conquered") is a collaborative project funded under the EU 7th Research Framework Programme. It is aligned to the strategic objective 1.4—Secure, Dependable, and Trusted Infrastructures—defined by the European Commission in the FP7 ICT Work Programme Call.

The Future Internet will provide an environment in which a diverse range of services are offered by a diverse range of suppliers, and users are likely to unknowingly invoke underlying services in a dynamic and ad hoc manner. Moving from today's static services, future service consumers will transparently mix and match service components depending on service availability, quality, price and security attributes. Thus, the applications end users see may be composed of multiple services from many different providers, and the end user may have little in the way of guarantee that a particular service or service supplier will actually offer the security claimed.

Aniketos helps to establish and maintain trustworthiness and secure behaviour in a constantly changing service environment. The project aligns existing and develops new technologies, methods, tools and security services that support the design-time creation and run-time dynamic behaviour of composite services, addressing service developers, service providers and service end users.

4 About the Organizers

Figure 4.1. From left to right: Christina Hochleitner, Trenton Schulz, Susen Döbelt, Sandra Trösterer. Not pictured: Elke Beck, Marc Busch, and Manfred Tscheligi.

The projects had partners across Europe. What follows is a short biography of the organizers, split by organization. A picture of some of the organizers is in Figure 4.1.

Christina Hochleitner, Marc Busch, and Susen Döbelt are HCI researchers at CURE in Vienna where they are conducting research on security and privacy. They are engaged in the EU FP7 project uTRUSTit that is researching trust in connection with the Internet of Things.

Sandra Trösterer and Elke Beck are research fellows at the HCI & Usability Unit of the ICT&S Center of the University of Salzburg. They are engaged in the EU FP7 project ANIKETOS, investigating usability and user acceptance in the domain of secure and trustworthy composite services.

Trenton Schulz is a research scientist at the Norwegian Computing Center. He focuses on universal design of ICT and usability and is involved in looking at universal design and trust issues in the IoT with the uTRUSTit project.

Manfred Tscheligi is full professor for HCI & Usability at the ICT&S Center of the University of Salzburg and is directing CURE (Center for Usability Research & Engineering) in Vienna. In Salzburg he initiated and is directing the Christian Doppler Laboratory on Contextual Interfaces with the topic on contextual user experience. He has been involved in the organization of several conferences (e.g., CHI, ACE, MobileHCI, EuroITV, AmI, AUI). In recent years he organized workshops at IDC 2011, MobileHCI 2011, AUI 2011, INTERACT 2011, AmI 2011 and CSCW 2012.

5 Identifying Trust Strategies in the Internet of Things

by Trenton Schulz and Lothar Fritsch

Abstract

Users in the Internet of Things (IoT) use strategies to determine if they should trust a system or service. These strategies are not actively declared, but it can be useful to know which strategy is being used. We provide possible actions that users may perform when using different trust strategies and possible ways these can be captured for user studies.

Introduction

In the future, people will have many devices that communicate with other devices and the Internet. This Internet of Things (IoT) requires that users trust the things and the things' providers. Previously [1], we outlined strategies that were used for the Semantic Web [3] – a concept of sharing data across applications – and applied them to the IoT. Choosing the best strategy depends on the situation. Even with the strategies identified, a user does not consciously pick a strategy to deal with the uncertainty in the IoT. It might be useful to identify these strategies during user interviews, observations, or tests. We provide a short review of the trust strategies – including actions that users perform when using one of these strategies – and possible ways actions can be picked up.

Trust Strategies

The five trust strategies are: *optimistic strategy* – assume everything is trustworthy unless proven otherwise; *pessimistic strategy* – assume everything is untrustworthy unless proven otherwise; *centralized strategy* – trust information is managed through a central authority; *investigative strategy* – investigate agents to determine their trustworthiness; and *transitive strategy* – using networks of agents to determine the trustworthiness of other agents.

These strategies were originally developed for gathering data in the Semantic Web and deciding how to deal with the uncertainty of a source. These strategies are useful in other contexts (like the IoT) where users can run into lots of different devices and services that they may not know if they should be trusted or not.

We've speculated on ways these strategies can be used in the IoT [1] and discussed how the strategies can be simulated in a trust model [2]. Let's take a look at possible ways these strategies might be used by real users when confronted with IoT devices or services.

Looking for Trust Strategies

Each of these strategies, when executed by the user, has unique actions that can be observed to determine which strategy is being used. The following paragraphs list possible actions that can reveal what sort of strategy is being used. We also provide suggestions for the detection of these actions.

Users employing the optimistic strategy tend to try things out while they feel that security and privacy risks are things that happen to other people. They will not do things that they know are not safe, but, in general, when presented with a choice to do something new, optimistic strategy users will choose to do it without much contemplation as long as there are no known, strongly negative facts.

It should be possible to notice this strategy. Recording the time users take to make a decision can pick this up. Video recording of interactions or an eye-tracker can help clarify this. For example, when using a mobile device, you can find out if users are actually reading information before they make a decision or if they just tap through policy information, security warnings, and configuration screens to move on to the main task.

Pessimistic strategy users are a mirror image of the optimistic strategy users. They only go to places that they trust. When given a choice to do something new, these users will choose not to do it without much thought or risk assessment. The axiom of the pessimistic strategy is the expectation of untrustworthiness. Pessimistic strategies are chosen based on a basic negative expectation due to either personal attitudes or negative information about the system or product the user is facing.

Since the pessimistic strategy mirrors the optimistic strategy, similar actions are observable. The amount of time for the user to make a decision is still significant. Though the user is making a different choice, the amount of time to make a decision is similar: the user is reflexively choosing to not trust something. An eye-tracker and video recording can also help confirm this strategy. As in the example above, pessimistic strategy users will still not read the detailed information provided by the system vendors or service providers.

Users employing the centralized strategies delegate parts or all of their decisions on whether or not to trust something to a trusted entity (trust rooting). The canonical example is the Public Key Infrastructure (PKI) for Secure Socket Layer (SSL) certificates for websites. Other examples include only using things from a trusted provider (e.g., apps only from a specific app store) or only browsing a regulated Internet within a subjectively trustworthy walled garden.

The centralized strategy does not present as many cues that can be picked up during a user interface (UI) test. It may be possible to see if a user takes the time to examine certificates that are issued for a particular device or service, or where something comes from, but if it is obvious whom the provider is, there might not be any cues and it could be misdiagnosed as an optimistic or pessimistic strategy. A better way to discover if the centralized strategy is used is to ask questions to users about what sort of applications they

run, why these specific programs, what sort of things they consider when doing something new, and whether or not they modify their devices to run any software (sometimes referred to as *jailbreaking*). If users' answers point to them relying on specific authorities, it is very likely they are using the centralized strategy. Trust anchors are often preinstalled on devices such as smart phones. They can be strongly correlated with brand names, large stakeholders, or regulatory frameworks. Any survey activity on the centralized strategy should take awareness or unawareness about the implicit trust anchors into account.

The transitive strategy involves a user contacting peers for the trust question. These peers may contact other peers and the final decision is based on the peers' answers. This strategy is similar to the web of trust that was first introduced by Zimmerman for Pretty Good Privacy (PGP) encryption [4]. The difference between this and the centralized strategy is that authorities in the centralized strategy are liable for the decisions and recommendations they make, whereas the transitive strategy is based on collected opinions with no direct liability.

If a user is consulting online resources or using social media to find opinions about a device or service, it is an indication that a transitive strategy is being employed. A question to ask users is why they trust using whatever they are using. If the answer is that it is what their peers are using, the transitive strategy is in use. Reliance on expert judgments, media exposure, the "crowd" using the same application, and personal contacts that use or recommend the application all contribute to the transitive strategy. Like the centralized strategy, it may be important to observe or ask other questions to make sure that consulting with peers is not part of an investigative strategy. We feel that an important difference from the optimistic and pessimistic strategies is that some form of communication and active information collection appear.

Users choosing the investigative strategy take time to do manual checking of a device or service to determine trustworthiness. These users don't necessarily settle on one answer either; they will also re-check again at a later time. It is up to the individual user to make the decision and not someone else.

There should be lots of observable signs to indicate users employing the investigative strategy. These users should be checking the services they are using. This can include: running software or other diagnostics to determine what a device or service does, talking to peers and experts, or checking the online community to find more information. They read policies, reflect on them, and employ conscious software configuration to use their conclusion on the system configuration. The investigative strategy may combine some techniques that are used in other strategies, so it may also be necessary to ask some questions about users' plans of attack when looking at a new device or service to confirm that this strategy is being used. A key thing to notice is if the user is trying multiple methods to triangulate and find a response. The responses and resulting actions might look very different from situation to situation.

Discussion

There is no strategy that leads to correct trust decisions in every situation. For example, an optimistic strategy is fine for situations where there is very little risk and the time required to do lots of other checks may be prohibitive. On the other hand, if there is a lot of risk and there is no other way of finding out information, a pessimistic strategy might be the best solution. Yet, a user only using the pessimistic strategy may find it difficult to accomplish tasks with new technologies and services. Users employing only an investigative strategy may tire of investigating every source, and centralized strategy users may be concerned about the central authority making a mistake.

Naturally, users pick a strategy that matches their goals and situation – likely constrained by time, background knowledge, education, value at stack, and risks involved. A user that is enthusiastic about a device may do a lot of research about it or just blindly trust in it; another user who is forced to use something may find any reason possible to not trust it. Being able to determine what strategy users employ at certain times may make it possible to make better decisions.

Future Work

Though we have listed ways to identify strategies, work needs to be done to design ways to capture them. This includes proper set up of equipment (e.g., video cameras and eye-trackers), and the design of questionnaire instruments. What questions need to be asked to identify clearly one of the strategies is yet to be developed. Other research opportunities can be finding out why users pick certain strategies and if there is any way to encourage them to pick better strategies for a situation. Finally, the isolation of trust signals that users react to while they employ the different strategies can be useful input to designers of software and systems.

Acknowledgements

This research is funded as part of the uTRUSTit project. The uTRUSTit project is funded by the EU FP7 program (Grant agreement no: 258360). Thanks also to Jan Zibuschka for providing feedback on an earlier version of this document.

References

[1] Fritsch, L., Groven, A.-K., and Schulz, T. On the Internet of Things, Trust is Relative. In *Constructing Ambient Intelligence*, R. Wichert, K. Laerhoven, and J. Gelissen, Eds., vol. 277 of *Communications in Computer and Information Science*. Springer Berlin Heidelberg, Berlin, 2012, 267–273.

[2] Leister, W., and Schulz, T. Ideas for a Trust Indicator in the Internet of Things. In *SMART 2012—The First International Conference on Smart Systems, Devices and Technologies*, W. Leister and P. Dini, Eds., IARIA (Stuttgart, 2012), 31–34.

[3] O'Hara, K., Alani, H., Kalfoglou, Y., and Shadbolt, N. Trust Strategies for the Seman-

tic Web. In *ISWC 3rd International Workshop on Trust, Security, and Reputation on the Semantic Web* (Hiroshima, Japan, 2004).

[4] Zimmermann, P. *The Official PGP User's Guide*. MIT Press, Cambridge, Massachusetts, USA, 1995.

6 Trust Implications for Universal Design of Social-Networking Applications

by Till Halbach Røssvoll

Abstract

Privacy-sensitive applications inside social networks require the trust of the user and all involved parts, such as banks and ID providers. This contribution discusses the consequences for the accessibility and usability requirements of such systems and presents a number of design principles.

Introduction

For architects and developers of the ever growing number of social networks and electronic services, access and identity management (AIM) is a natural part of the system design. AIM refers to techniques for determining and organizing the identity of a user in order to grant access to a service or data, or to authorize the execution of a task [4]. However, few of these systems pay attention to accessibility and usability issues [5]. In the context of ICT, accessibility describes the degree to which a solution is accessible for as many people as possible, and in particular those with impairments. Usability refers to the ease with which people can use a particular product or service. Researches have previously pointed out the need for inclusive identity management (IIDM) to rise the floor for virtually all users [2].

This paper discusses trust implications of privacy- sensitive services and AIM in the context of online services and social networks, where trust—in the most generic sense—is defined as the reliance of one entity on another entity [1]. It is organized as follows. First, the scope providing research project is introduced, followed by a description of the prototype application and a discussion of einclusion and trust aspects. Before the paper concludes, a number of trust establishing measures is presented as a checklist.

The PayShare application

The research project e-Me sets the context for this work. Its main goal is to provide new knowledge that can improve the usability and accessibility of AIM and authentication mechanisms in new social networks without compromising privacy, security, and avoiding to offend legal frameworks. In the course of the project, the example application PayShare has been developed. This prototype is a means to test design principles, user interface, and system functionality.

PayShare can be described as an online payment service. Upon registration, which basically requires the user's acceptance of the Terms and Conditions of the service, users can file payment claims for entire parties, assuming all party members are also connected on a particular social network online. For instance, consider a group of friends out to travel. One of them, here called creditor, pays for the travel tickets of the entire party and files claims against all party members, here referred to as debtors, in PayShare. The debtors then get notifications that there are open claims that they have to pay, and the creditor can conveniently track any payment progress. Payments can be made directly in the PayShare service, to/from a virtual wallet in form of so-called credits, or to/from an account in a trusting bank. There is the possibility to transfer money from the bank account to the virtual wallet.

The security of payments is ensured by several measures. There is a user-defined threshold for the payment amount. If the amount is above the threshold, an additional authentication of the user is required to authorize payments. As such, users are enabled to put a price at the convenience of not having to go through an authentication process for small-amount payments. Payments with an amount below the threshold are one- click payments. Authentication is delivered by an OpenID provider, which has the advantage that only a single password has to be remembered by the user, even for a variety of applications and web sites. Data from any authentication, be it login to the social network or authorization of a payment, expires according to a user-defined time span for authentication validity. This measure aims at avoiding frequent cumbersome authentications as the user's ID is remembered for this specific time span. Consequently, an authentication process is only invoked when the payment's amount is above the threshold, and when the last authentication has been too long ago.

E-Inclusion

As mentioned before, the project's focus is on inclusion aspects of the solution. Its target groups consist of users with various impairments, and the elderly.

Acknowledged impairments are cognitive challenges such as dyslexia and dyscalculi, orientation, and memory problems, sensory challenges like vision and hearing reduction, and motor challenges like trembling hands. Elderly users are likely to have a combination of impairments. However, apart from these focus groups, PayShare is required to be universally designed, meaning that it can be used by virtually all persons.

The starting point for the development of a highly usable and accessible prototype was a literature review on the field of accessibility and usability issues of personal identification systems [3], recommending— among others—an open and universally designed solution with an accessible, adaptive, and personalized multimodal user interface, a minimally exposed user profile with reasonable defaults and opt-ins, and combined with privacy-enhancing technology. With this in mind, two hypotheses were set up: First, the majority of users is suffering from having to handle too many user names and passwords for authentication. And second, the majority of current authentication mechanisms is not accessible to users with impairments. The solutions provided by PayShare are: OpenID to

cut down the numbers of service accounts to remember for the user, and several OpenID login alternatives, namely password, series of pictures, series of sounds, pattern, and personal question.

Apart from login, the system's inclusiveness is met by a number of measures concerning universal design. For instance, the user interface is tailored to the needs, preferences, and context of the respective user by means of a user profile, satisfying major parts of the first requirement from the literature review.

Trust Implications

As a payment service that voluntarily relies on OpenID for authentication and is linked to a bank account, there is a chain of trust from the bank (the trustor) to PayShare (the trustee) and the OpenID provider. The bank has, as minimum requirements, to trust that all virtual credits are safe and properly handled with the service, all payments are correctly executed, and that personal data are handled in a confidential way. The same applies to the trust chain from the user to PayShare, the OpenID provider, and finally the bank.

Is is argued here that especially impaired users need particular measures to develop the same degree of trust like the average user to make up for the impairment. For instance, a blind person who is enabled to use an audio-based authentication scheme will have more trust in such a system that accounts for the user's preferences than systems that only offer visual CAPTCHAs. Similarly, a person with orientation and problem solving problems is likely to develop more trust in a system showing explaining messages about what is about to happen on the current screen than systems that do not have the same degree of usability. The following design principles were applied in PayShare to increase the user's trust into the service. They are deliberatively held as generic as possible to make them applicable for electronic services in general. Basically, it all boils down to giving the user full control over the service, and enabling the user to make informed decisions.

- Require extra confirmation before critical actions such as claim deletion
- Show concise and comprehensive system messages that explain the general context. (what the user is about to do), the concrete task at hand, the requirements needed, such as PIN code calculator, and the concrete instructions.
- Show brief and comprehensive error messages with both concrete and general help information, and directions to a human contact.
- Offer a dashboard view to ease overview gaining.
- Offer multiple easy-to-find links to the profile settings.
- Offer several easy-to-find links to Terms and Conditions.
- Make all user settings non-mandatory.
- Only expose particular profile settings on demand.

- Use safe defaults for all user profile settings.
- Offer several easy-to-find possibilities to delete the user/profile.
- Make as many user actions as possible reversible.
- Offer multiple possibilities to delete user data.
- Anonymize all user data that are impossible to delete.
- Only show information relevant in a specific situation.
- Offer an archive with previous events and actions, comparable to a system log.
- Offer a multitude of authentication methods.
- Hold the design of an OpenID server different from the design of the service to illustrate the mechanisms invoked during an OpenID authentication.
- Honor accessibility and usability standards.

Evaluation and Testing

So far, the PayShare application has been evaluated by expert users and personas, and in scenario walkthroughs, while testing with a number of users of the target groups is on the way.

Conclusion

User control and information are crucial to achieve a high degree of trust of the user to the service. There is a connection between eInclusion and trust in terms of the fact that a high degree of accessibility and usability empowers the user in certain situations to use the respective service at all. In other situations, it increases the user's control or feeling of control and thereby the user's trust. The perception of increased trust is not only applicable to users with impairments but rather all users, as it is widely recognized that e-inclusion measures for particular focus groups generally increase the service's usability for everybody.

Acknowledgements

This work is part of the e-Me project, which is funded by the Norwegian Research Council under the VERDIKT program. It has grant no. 201554.

References

[1] Bamberger, W. Interpersonal Trust – Attempt of a Definition. Tech. rep., Technische Universität München, Munich, Germany, 2010.

[2] Fritsch, L., Fuglerud, K. S., and Solheim, I. Towards Inclusive Identity Management. *Identity in the Information Society 3*, 3 (2010), 515–538.

[3] Fuglerud, K. S., and Røssvoll, T. H. Previous and Related Research on Usabil-

ity and Accessibility Issues of Personal Identification Management Systems , 2010. http://publ.nr.no/5371.

[4] Røssvoll, T. H., and Fuglerud, K. S. Usability and Accessibility of Personal Identification Management Systems in Electronic Services. In *eChallenges e-2011 Conference Proceedings*, P. Cunningham and M. Cunningham, Eds., IIMC International Information Management Corporation (2011).

[5] Sauer, G., Holman, J., Lazar, J., Hochheiser, H., and Feng, J. Accessible privacy and security: a universally usable human-interaction proof tool. *Universal Access in the Information Society 9*, 3 (2010), 239–248.

7 Establishing Trust in Industrial WSN

by Basil Hess, Felix von Reischach, and Laura Gheorghe

Abstract

This paper considers trust from the perspective of industrial Wireless Sensor Networks (WSN). In this context, we present scenarios such as monitoring industrial processes, and identify the role of trust with its different entities that act as trustor and trustee. We present an approach to establish trust in a mostly automated manner with minimized user-interaction. Since even in this approach, user-centric challenges remain, we add a discussion on the user-perspective and highlight the potential to combine a technical project like TWISNet with HCI research.

Introduction

In industrial environments there are often thousands of sensors deployed that generate and exchange a vast amount of data. Manually managing each sensor and assessing their credibility is not feasible.

One of the scenarios considered in TWISNet [1] is the manufacturing process for airplanes [6]. Automated process steps like testing of the airplane flaps require the establishment of temporary exclusion zones, where no worker must enter. The sensor network is used for keeping workers away from the exclusion zones by tracking their position. Automatic verification of the exclusion property is here crucial for workers' safety.

Another scenario relates to workers in environments that expose them to radiation, like in certain areas of nuclear power plants. Health and legal regulations require the workers' radiation exposure to be continuously monitored, so that it is ensured that the cumulative radiation does not exceed a certain level. Radiation sensors are attached to workers in order to avoid radiation exposure. Besides reliable measurement, privacy policies on health-related data require that the data is kept confidential.

A third scenario is smart metering of the energy consumed by individual electric devices. Visualized data helps home users to become aware of the energy efficiency of their devices, and aggregated data will be routed to the energy provider. For privacy reasons, it has to be ensured that the energy provider doesn't individually profile its customers.

1. TWISNet (Trustworthy Wireless Industrial Sensor Networks) is an EU FP7 security and trust project. It addresses the security concerns raised by the deployment of Wireless Sensor Networks (WSNs) into industrial environments. The goal of the TWISNet project is to provide a platform for an efficient, secure and reliable integration of sensor networks into large scale industrial environments. Started in 2010, TWISNet involves seven European partners from academia and industry. URL: www.twisnet.eu

The approach employed by TWISNet to establish trust is to provide an architecture that addresses the threat and attack models of the scenarios. Motivated by the complexity of WSN, the goal is to minimize user- interaction. For example, in the case of compromised security material, the architecture aims to automatically adapt to this condition and re-configure the WSN. Sensor networks may use trust and reputation models to assess the validity of sensor data. Considering this automated approach, the user-perspective is beyond the main focus. Considering the three scenarios, we however observe that different groups of users are involved in trust relations with the WSN. Motivated by this, we consider it as worthy to seek feedback from the HCI community: (1) by discussing the role of trust in WSN, (2) by explaining how TWISNet addresses trust in its architecture and (3) by discussing challenges that arise from a user-perspective.

Role of Trust in Wireless Sensor Networks

Let's consider a definition of trust by Castelfranchi and Falcone [3]:

> Trust is the subjective probability by which an individual A, expects that another individual, B, performs a given action on which its welfare depends.

Adapted to the case of the TWISNet scenarios, A would be the trustor and could be:

- The worker or employee of a company that is monitored by the WSN, or that depends on certain conditions being monitored at the workplace.
- The manager responsible for the worker's safety, or for seamless running infrastructure.
- The legislation that imposes health regulations.
- Home users that benefit from a service, like in the smart metering scenario.

B would be the trustee and could be

- The employer of the worker
- The company that provides services to the customers that involve sensors (e.g., electricity provider)

In the WSN case, there is no direct trust relationship between A and B. The TWISNet architecture acts as agent on behalf of B to provide technical solutions to establish trust. Such a relationship can probably best be described by agency theory (e.g. [1, 2]), also known as the principal-agent problem: The WSN architecture should act on behalf of the user or worker to ensure security and privacy properties. On the other hand, it is the employer or a company's duty to implement the security infrastructure, which could potentially lead to conflicts of interests and selfish behavior. To mitigate this risk, it is important to provide a transparent architecture for security in WSN that has been independently developed and publicly disseminated.

In the following section, we summarize the technical measures to establish trust.

Technical Measures to Establish WSN Trust

The TWISNet approach for establishing trust can be classified in four principles: (1) by trust models, (2) by architecture, (3) by cryptography and (4) by demonstration.

Trust Models

Using trust models, it should be possible to quantify trust in the WSN. On one hand, "trust metrics" are assigned to sensor nodes, depending on their reputation in delivering data and on previous behavior. On the other hand, sensor data is assessed for trustworthiness. This is done by defining a sensor data life-cycle from sensed, routed, aggregated to delivered states. The quantification can be probabilistic-based [5], subjective-logic-based [4] or information-theoretic- based [7].

Architectural Design

The architecture is designed to be composed of modules, where each of them fulfills parts of the security requirements. There are modules that allow (1) automatic reconfiguration (2) managing identities, authentication and access control, (3) shared information access, (4) guaranteed availability, (5) dynamically adapting security mechanisms, (6) failure detection and data assessment, and (7) mediation between WSN and end-users.

Cryptography

End-to-end security is an important concept for enforcing data confidentiality, integrity and availability. Data is secured when sent by the node and will eventually only be decrypted at an authorized end- point (e.g. a protected health-database).

Demonstration

To show the applicability of the TWISNet concept, a combination of simulations and real-world deployments will demonstrate effectiveness of the implementation, as well as proving resistance against attacks.

Discussion: Challenges from a User Perspective

Despite the main scope of TWISNet to provide an architecture that allows establishing trust with minimal amounts of user-interaction, trustworthiness is finally a user-centric concept. We would therefore like to discuss user-centric points that could in the future potentially lead to an extended research agenda.

Architecture as Trusted Agent

As described in the section that presents the role of trust in WSNs, the goal of the TWISNet architecture is to establish trust for users on behalf of a trustee. The security architecture can be verified by independent domain experts. This might however not be feasible by the users of the system. A similar problem exists, for example, in online banking. The complex mechanisms involved to establish secure transactions are likely not to be understood by average users. Well-known labels or the "secure connection" label in web browsers abstract the complexity and deliver easy hints that establish trust. Such abstrac-

tions that guarantee security are harder to deliver in WSN, where users do not necessarily explicitly interact with the system.

The resource-constraints of WSNs lead to certain security-efficiency tradeoffs: Achieving strongest security is often not possible because of processing power, memory and battery constraints. How this affects user-trust could be further investigated.

User notifications and data trustworthiness

While most of security-related tasks can be automated, some groups of users eventually have to be notified in case of critical events. Detection of critical events involves solving a statistical testing problem that potentially leads errors of type I and type II. There is a trade-off between delivering false alarm and missing to detect critical events. Adjusting the testing thresholds should involve performing user-studies, since both false positives and false negatives are likely to diminish trust in the system. Also the deployment of techniques that automatically assess data trustworthiness could likely benefit from the involvement of user-studies for assessing the quality of the trustworthiness.

These examples could bear potential for introducing HCI research to otherwise technical security and trust projects. We believe that further discussions with the HCI community could be beneficial to show how projects like TWISNet could benefit from HCI, and vice versa.

Acknowledgements

This work is supported by TWISNet under grant agreement FP7-ICT-258280.

References

[1] Alchian, A. A., and Demsetz, H. Production, Information Costs, and Economic Organization. *The American Economic Review 65*, 5 (1972), 777–795.

[2] Bahli, B., and Rivard, S. The information technology outsourcing risk: a transaction cost and agency theory-based perspective. *Journal of Information Technology 18*, 3 (Sept. 2003), 211–221.

[3] Castelfranchi, C., and Falcone, R. Principles of trust for MAS: cognitive anatomy, social importance, and quantification. In *Proceedings International Conference on Multi Agent Systems (Cat. No.98EX160)*, IEEE Comput. Soc (Paris, 1998), 72–79.

[4] Dempster, A. P. *Classic Works of the Dempster-Shafer Theory of Belief Functions*, vol. 219 of *Studies in Fuzziness and Soft Computing*. Springer Berlin Heidelberg, Berlin, Heidelberg, 2008.

[5] Gomez, L., Laube, A., and Sorniotti, A. Trustworthiness Assessment of Wireless Sensor Data for Business Applications. In *AINA* (2009), 355–362.

[6] von Reischach, F., Oualha, N., Olivereau, A., Bateman, D., and Slusanschi, E. Scenario Definitions and their Threat Assessment, TWISNet Deliverable 2.1. Tech. rep., SAP, 2011.

[7] Zhang, W., Das, S., and Liu, Y. A Trust Based Framework for Secure Data Aggregation in Wireless Sensor Networks. In *2006 3rd Annual IEEE Communications Society on Sensor and Ad Hoc Communications and Networks*, vol. 1, IEEE (Reston, VA, 2006), 60–69.

8 Understanding Trust in the Context of Personal Information Systems

by Caio Stein D'Agostini, Marco Winckler, and Cédric Bach

Abstract

This paper is concerned with the representation of trust in Personal Information Management Systems (PIMS). Originally, PIMS have been conceived for helping users store personal information for private use. However, most of Web applications (ex. social networks, web services and applications) require personal information, turning recent PIMS into tools for sharing information with third-party applications. Since trust can affect the users' decisions to share their information, it is important to address it. Trust affects i) how users perceive/feel the PIMS system, ii) how information is collected, stored into PIMS and later shared with other users or systems. This works tries to associate elements from different definitions of trust to the types of interaction between parties involved with Personal Information Management. We present some scenarios describing data exchange between PIMS and third-party applications. Our ultimate goal is to discuss the complexity of trust and how it is permeable through the information flow.

Introduction

In recent years the access to internet and mobile devices improved the users' capabilities for managing large information sets needed in everyday life. Part of that information refers to personal data that users might decide to share or not through their relationships with other users (e.g., social networks) and applications (e.g., e-government services). Those decisions depend on whether they trust or not the parties receiving/giving the information.

Trust is often described with subjective concepts, which depends on the context it is used, meaning some aspects may be more relevant on certain contexts than others. Consequently, there are multiple models and definitions for describing trust. The diversity of definitions relates to Personal Information Management (PIM) because the users' information that is forwarded and re-shared goes beyond the boundaries of individual systems. Also, users are influenced by other information, such as reputation, recommendation, certification, etc. Thus, there can be more than one single relevant definition of trust involved when developing a Personal Information Management Systems (PIMS).

This work proposes to associate the user's interactions to events. The events can be evaluated by the user regarding how the user trusts the involved parties or information. The

Work	Subject	Dimensions
[3]	Software Systems	**Affective Trust** (emotional state) **Cognitive Trust** (system's state, e.g.: program is running/frozen, network speed is normal/slow)
[5]	Automated Systems	**Performance** (system's capacity for helping the user) **Process** (use of adequate algorithms) **Purpose** (intentions of the system designer)
[1]	Personal Relations	**Competence** (capability, reliability and confidence to perform according expectations) **Benevolence** (genuine interest in the other's welfare)
[2]	Consumer-eCommerce	**Integrity** (honesty and promise keeping) **Competence** (ability to do what is needed) **Benevolence**(care and motivation) **Predictability** (consistency of behavior)

Table 8.1. Trust and its dimensions

result is a history that explains past interactions, can be revisited either by systems or by the user, and used to assign a trust value for current actions based on past experiences.

Definition of Trust

Trust is a concept present on different types of applications, for different purposes. Because of that, users give different degrees of importance for different aspects of trust, depending of the application context. Table 8.1 list some definitions of trust for different scenarios, breaking them into their respective trust dimensions.

A trust dimension is related to characteristics used to evaluate the trustee's trustworthiness [1]. Dimensions are composed of antecedents [5], which are individual elements that can be evaluated regarding their quality and whether those characteristics are present or not (e.g.: verify if the trustee has a certification (antecedent) in order to evaluate its competence (dimension)).

The user's trust depends on the user's trusting beliefs towards the dimensions that are relevant to the current context. Trusting belief is the trustor's perception that the trustee has the dimension's characteristics [2]. A user can belief (a positive perception) or it can have disbelief (a negative perception). However, trust is not a static value; instead it is **dynamic** and has to be gradually constructed [2]. Because of the possibilities that the user has never interacted with the trustee, has no knowledge about it or has ceased to interact for a significant amount of time, it is also necessary to consider **uncertainty** as a possible value for a trusting belief [4].

When a system is built to work on specific, well know scenarios, domain specif trust definitions are enough. What makes PIMS more complicated is that trust becomes subjective as the user's personal information can be used **across the boundaries of several systems** [6], subjected to multiple trust definitions. Consequently it is difficult to predict all possible uses for the user's information or to have immediate information regarding

all antecedents the trustor considers relevant for a given situation.

PIMS and Information Sharing

This section described the relation of trust and PIMS. In particular, how they can use PIMS to store, organize and share their personal information. We break PIM in the following scenarios:

i)The user stores the personal information on the PIMS ('*Provider*') and trusts the information integrity. The user trusts the PIMS to store the personal information.
ii) The PIMS publishes/discloses the stored information to other users and services ('*Consumer*') according to certain conditions of use (use conditions, conditions of use, etc.). The user trusts the exchange between PIMS and service is according to the conditions of use.
iii)The user's information is used by the consumer, either accessed from the PIMS or directly shared by the user (without the PIMS). The user trusts information is not disclosed or used misused.

Figure 8.1 illustrates them. The first part, '*Information Provider*', refers to the user and to his/her PIMS. The second part, '*Consumer*', refers to the party (system or other user) the user share his/her information with. It can even be another PIMS, if it is consuming the user's personal information. Finally, the third part, '*Other*', refers to people, institutions, organizations and other systems the user know about and, although they do not provide or consume the user's personal information, they can affect the user's trust. This influence can come from relations of reputation, recommendation, certification, etc. with the consumer.

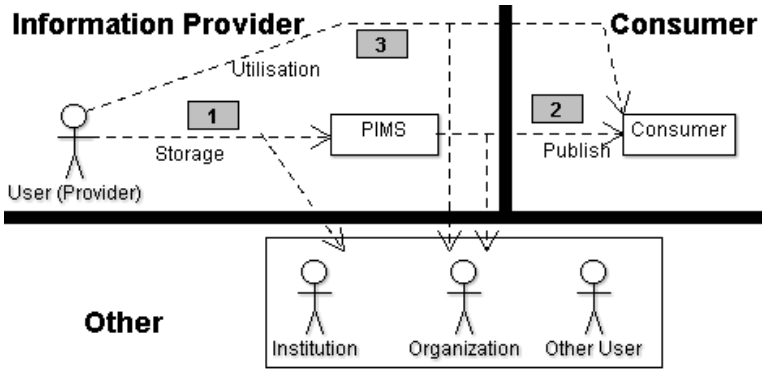

Figure 8.1. Breaking up trust for PIMS.

Temporal Aspects of Trust

Since the user's trust is constructed or degraded because of information and experiences the user collects along multiple interactions, **we consider managing trust using events**, as modeled in Figure 8.2.

Trust is a relation that has a trustee ('*Trustee*') and a trustor (an instance of '*Party*'; not in the diagram), which performs some action (on the context of PIMS, the action ('*Action*') is performed with the personal information ('*Information*')).

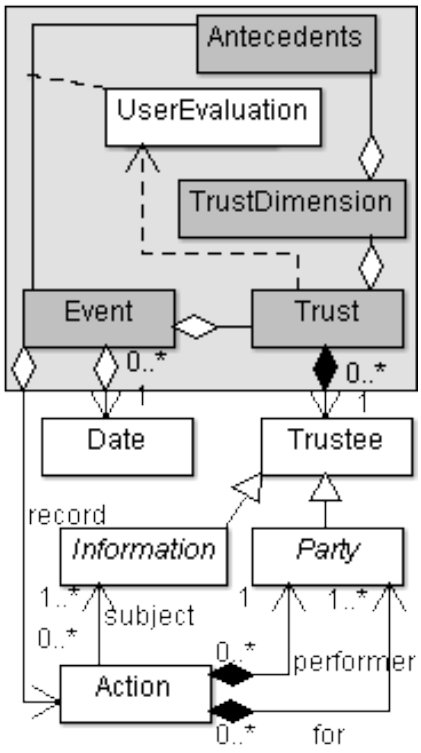

Figure 8.2. Trust associated to events.

Using the idea of trusting beliefs, when starting to build trust, each dimensions starts with a high level of uncertainty, which is replaced by belief or disbelief based on the user's feedback or recommendations. For each interaction, belief values are stored on the respective event. The overall trust can be calculated by leveraging the user's beliefs from previous events relevant to the user's context (which can be done by searching for common antecedents on the user's history of events); the older the event is, the smaller its contribution (Figure 8.3). If the user stays long periods without interacting with the trustee, the system can assign the belief as uncertain. The use of uncertainty as a possible value together with the "forgetting" of past interactions allows the system to model lost trust, regained trust, doubt, etc.

The different dimensions ('*TrustDimension*') depend on antecedents ('*Precedent*'). Those antecedents come from previous events, modeled in Figure 8.2, such as meeting someone, having previously performed an action, etc.

This solution allows users and systems to revisit previous events and experiences and understand how the beliefs on different dimensions of trust were built or degraded. It also allows the systems to handle trust as dynamic value that is not coupled to a single action. Those capabilities are independent of domain specific definitions of trust,

Discussion

Trust in undoubtedly relevant for enriching the human-computer interaction, even more when the interaction involves multiple systems or organization, such as the case of PIMS. While there might be very precise trust definitions for specific domains, they are not

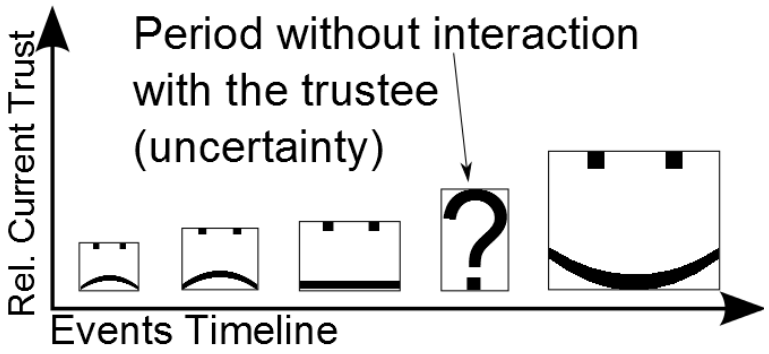

Figure 8.3. Contribution of past events' trust to current trust.

necessarily easy to adapt to different scenarios. We propose to manage trust across its multiple definitions as a series of events which can be revisited by the systems and user.

References

[1] Cho, J. The mechanism of trust and distrust formation and their relational outcomes. *Journal of Retailing 82*, 1 (2006), 25–35.

[2] Harrison McKnight, D., Choudhury, V., and Kacmar, C. The impact of initial consumer trust on intentions to transact with a web site: a trust building model. *The Journal of Strategic Information Systems 11*, 3-4 (2002), 297–323.

[3] Hasan, Z., Krischkowsky, A., and Tscheligi, M. Modelling user-centered-trust (uct) in software systems: Interplay of trust, affect and acceptance model. *Trust and Trustworthy Computing* (2012), 92–109.

[4] Ray, I., Ray, I., and Chakraborty, S. An interoperable context sensitive model of trust. *Journal of Intelligent Information Systems 32*, 1 (2009), 75–104.

[5] Söllner, M., Hoffmann, A., Hoffmann, H., and Leimeister, J. How to use behavioral research insights on trust for hci system design. In *Proceedings of the 2012 ACM annual conference extended abstracts on Human Factors in Computing Systems Extended Abstracts*, ACM (2012), 1703–1708.

[6] Tomkins, C. Interdependencies, trust and information in relationships, alliances and networks. *Accounting, Organizations and Society 26*, 2 (2001), 161–191.

9 Older people's strategies for building trust in online communities through an ethnographical lens

by Valeria Righi, Andrea Rosales, Sergio Sayago, and Josep Blat

Abstract

The paper presents key results of an ethnographical study we conducted with 55 older people (aged 59-80) over 18 months while participating in online communities. The results show that trust is very important for this user group. Privacy and concerns about misuse of personal information are important elements of trust for them, and closed social circles and everyday trusting strategies are key ingredients of their virtual and face-to-face trust building processes.

Introduction

Much of previous HCI research on trust has focused on e-commerce and been conducted with ordinary HCI users (i.e. young and adult people). In our research, we are looking into trust building in non-ecommerce websites with an ever-growing sector of the population, older people (60+). We aim to understand their trust building process in online social networks and how it can be facilitated with improved Social Network Sites (SNS). We present key results of an 18-month ethnographical study of older people's use of popular SNS we conducted to this end. The study is framed in the Life2.0 project1, partially funded by the EU, aimed at making the local network of older people's social interactions more visible amongst themselves and their social circles through geo-located online services.

Related Work

The bulk of research: trust in e-commerce

Trust has largely been studied in e-commerce. Much of this research has focused on determining web-based elements, such as graphical design and information quality (e.g. [1]) and important company-based qualities, for instance, reputation and external guarantees (e.g. [5]), which influence trust building with clients. We have been addressing web-based elements, as well as motivations, social practices and human actors involved in the trust building process, which are important aspects of the second and current wave of HCI research [3], in online communities.

Trust in Online Communities

We consider that Tricia Wang's distinction between social circles and social networks in Chinese online communities can help us understand trust building in our research. According to Wang [6], social circles consist of people we already know (e.g. friends, relatives) and social networks of people we do not know (yet). Thus, "social circles build on existing relations of trust, and social networks build out new relations of trust" ([6, minute 15]). This implies that trust in online social networks is created through "trust-exploring-practices", and in our research we aim to understand the practices conducted by older people.

Trust, online communities and older people: lots to do

Whilst previous studies of trust with older people have largely focused on exploring the extent to which they trust technologies embedded in caregiving devices (see [4] for a review), there seems to be a lack2 of research into trust in online communities with older people, despite the increasing adoption of SNS amongst the older population and the importance of trust in social interactions [2].

Our study: setting, participants and methods

We have been conducting our ethnographical study in Àgora, a 26-year-old adult highly participatory educational centre in Barcelona (Spain). Our study adopted a classical ethnographical approach, i.e. we conducted in-situ observations and conversations over a prolonged period of time (18 months) with a group of 55 older people (aged 59–80). All the participants were familiar with basic ICT-tasks and 45% with Internet- related tasks. They reported using the computer at least once per week. We conducted the observations and conversations weekly, while the members of our user group were using different community-based technologies, such as Facebook, YouTube, Picasa, Google Maps, Twitter and the Life2.0 community platform3, and other more common ones, such as e-mail and picture-editing tools, in different ICT courses in the centre. This resulted in over 230 hours of fieldwork. We also set up a Facebook Group in one of the courses, establishing Facebook friendship with 41 older people. Reading their posts and flow of messages, and talking with them allowed us to begin to make sense of the relationship between older people and SNS. We analysed our field notes and the content the participants of the Facebook group posted in their online social network by conducting qualitative data analysis techniques (open, selective and axial coding).

Findings

The nature of trust concerns in online communities

One of the main concerns of our participants is whether the information they post/share in online communities, such as their photos, e-mail addresses or personal videos, can be accessed by people they do not know (or do not want to share with) and that can potentially make a bad use of it, e.g. sending spam e-mails with viruses. At the end of a course session, they also remove any personal documents they put on the computers, which are

used by different people, as "I don't want people I don't know to look at my things". Privacy, unknown people and the use they can make of the personal information seem to be three key factors in the definition of trust for this group. The complexity and constant evolution of tools to manage privacy settings in online communities (e.g. in Facebook, deciding who can read the posts) makes it difficult for our participants to use them effectively. Instead, they prefer using the private message functionality in SNS, since, in their opinion, it is similar to the e-mail tools they use.

Trusting the technologies or themselves using them?

Our participants did not show any concerns in trusting the technologies4 they were using. They often pointed out that these technologies do well its job and that they were the ones who make mistakes. This opinion influences how they participate in online communities, especially when they are learning to use them, e.g. in Facebook, they were often afraid of making mistakes which could result in an unwanted sharing of personal information. Trusting their ability to use the technology is the first step they have to take to start to participate in online communities.

Relying on their social circles to trust strangers

Our participants are willing to engage in online communities recommended by trusted people, e.g. family members and friends. For instance, a participant reported having joined a Facebook Group because a friend had recommended it to him. Another participant became a fan of the Facebook page of a local association because she knew the association and two of its members. These examples show that trust in online communities is built by this user group through closed social circles, mostly in face-to-face interactions.

Everyday trust building strategies go online

Gathering information about an unknown person by asking people they know in their neighbourhood or relying on information provided by trusted sources, such as local associations, are everyday trust building strategies adopted by our user group when participating in online communities. For example, our participants considered that a trusted member, e.g. a local association, to whom they could report bad behaviour or ask for further information about others members, would be useful in order for them to trust users of the mutual help service provided by the online Life2.0 platform.

Indirect network ties increases distrust

Our participants find it difficult to understand the message flow through direct (i.e. friends) and indirect (i.e. friends of friends) network ties. Whereas direct network ties are trusted, indirect ones are not. Our participants did not expect to be able to read in their News Feed comments made by unknown people (i.e. friends of their friends) or be encouraged—by the system—to add people they did not know to their friends' list. These indirect ties raised privacy concerns amongst our participants, i.e. can unknown people read my posts?

Discussion and plans for future work

We considered that going beyond identifying trust-cues in websites was worthwhile to start to understand trust in online communities with older people. Our results suggest that privacy control and concerns about misuse of personal information are important elements of trust for this user group, and that closed social circles and everyday trusting strategies are key ingredients of their virtual and physical trust building processes. Our next step is to understand trust further. To this end, we will conduct traditional and online ethnographical research in different communities of older people, to deepen and widen the data collected thus far. We will also conduct co-design with them, which should enable us to discuss implications for designing SNS which support and enrich much better their trust building experiences.

Acknowledgements

We are indebted to our participants for their collaboration in our research. This work has been partially funded by Life 2.0: *Geographical positioning services to support independent living and social interaction of elderly people* (CIP ICT PSP-2009-4- 270965).

References

[1] Beldad, A., de Jong, M., and Steehouder, M. How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust. *Computers in Human Behavior 26*, 5 (Sept. 2010), 857–869.

[2] Blanchard, A. L., Welbourne, J. L., and Boughton, M. D. A Model of Online Trust. *Information, Communication & Society 14*, 1 (Nov. 2010), 76–106.

[3] Bø dker, S. When second wave HCI meets third wave challenges. In *Proceedings of the 4th Nordic conference on Human-computer interaction changing roles - NordiCHI '06*, ACM Press (New York, New York, USA, Oct. 2006), 1–8.

[4] Frederick Steinke, Tobias Fritsch, and Lina Silbermann. A Systematic Review of Trust in Automation and Assistance Systems for Older Persons' Overall Requirements. In *eTELEMED 2012, The Fourth International Conference on eHealth, Telemedicine, and Social Medicine*, IARIA (Valencia, Spain, 2012), 155–163.

[5] Shneiderman, B. Designing trust into online experiences. *Communications of the Acm 43*, 12 (2000), 57–59.

[6] Wang, T. Dancing with Handcuffs: The Geography of Trust in Social Networks. In *Lift 12 conference, Geneva, Switzerland* (2012), 22–24.

10 Integrating E-Commerce and Social Engineering Perspectives on Trust in Online Communication

by Thomas Pfeiffer, Michaela Kauer, and Ralph Bruder

Abstract

Currently, interpersonal trust in computer-mediated communication is a research topic for e-commerce as well as usable security researchers. While the e- commerce researchers focus on gaining warranted trust, usable security researchers focus on preventing misplaced trust, in order to protect users from social engineering attacks. In this paper an approach to integrate findings and theories from both fields is proposed in order to create a complete model for predicting trust in electronic messages or websites, whether they are authentic or not.

Introduction

Trust plays an important role in digital environments. We have identified three different kinds of trust relevant in digital environments, each with a different pair of trustor and trustee: **Trust networks** [8] attempt to model interpersonal trust, with both trustor and trustee being nodes in a network. There, a trustor assigns a numerical value of trust to a trustee. This trust is then propagated across the network and used autonomously by a computer system e.g. to make recommendations to users. Those users however will only trust these recommendations if **they trust the system** (the second important kind of trust) producing them, believing that its algorithms are correct and not susceptible to manipulation. This paper focuses on a third kind of trust: **Interpersonal or organizational trust in computer-mediated communication**, a person's trust in another person or organization based on electronic messages. This topic is currently being investigated mainly by researchers from two disciplines: E-commerce and usable security.

We will give an introduction to the research on the subject from both fields in the next chapter, before outlining an approach to combine the research from both fields into an integrated understanding of interpersonal trust in computer-mediated communication. The paper closes with an outlook on future research.

Definitions

The following are useful definitions for the rest of the paper.

Social engineering According to Goodchild [7], "...the art of gaining access to build-

ings, systems or data by exploiting human psychology, rather than by breaking in or using technical hacking techniques."

Phishing "act of sending e-mail that purports to be from a reputable source, such as the recipient's bank or credit card provider, and that seeks to acquire personal or financial information. The name derives from the idea of 'fishing' for information." Taken from [2].

Trust (e-commerce) According to Harrison McKnight et. al [9], "...a multi-dimensional construct with two inter-related components— trusting beliefs (perceptions of the competence, benevolence, and integrity of the vendor), and trusting intentions—willingness to depend (that is, a decision to make oneself vulnerable to the vendor)."

Online trust problems (usable security) According to Kumaraguru et. al [12], online trust problems are, "...those that arise when dichotomies between signals and underlying states can affect the user's decisions and well-being, and when attackers can affect signals, states, and decision processes."

Current Research Perspectives

The E-Commerce Perspective

Researchers in the field of E-Commerce have been studying trust in e-commerce websites extensively [1, 16]. They focus on trust-inducing aspects of websites, aiming to provide guidelines for creating e-commerce websites that gain visitors' trust. In this case, the trustee is the e-commerce vendor; the trustor is the (potential) customer.

Beldad et al. [1] have grouped the antecedents to trust found in the literature in three categories: customer- based (e.g. propensity to trust), website-based (e.g. design or security assurances) and organization-based (e.g. reputation or familiarity) antecedents.

Several models were proposed for the formation of trust in e-commerce vendors (e.g. [3, 14]). They usually differentiate between stages in the process (e.g. Deterrence-based, Knowledge-based and Shared identification-based trust [3] or exploratory vs. commitment stage [14]).

The Social Engineering Perspective

Whereas e-commerce researchers study factors influencing trust with the goal of eliciting legitimate trust in commercial websites, researchers in the field of usable security try to find out which aspects of a fraudulent online message or website (used for the purpose of phishing [2] or social engineering [7] in general) or of its recipient/user either elicit or prevent misplaced trust. This knowledge is then used to more effectively educate or warn users about these fraudulent emails or websites.

Experiments and interviews have shown the effect of aspects like content [4, 11, 13, 16], design [4, 11, 13, 16], third-party seals [13, 16], URLs [4, 11, 16] sender's email address [10, 11], brand/reputation [12, 13] or presence of security/privacy assurances [13] in emails and websites on either user's likelihood to click links in emails/enter information

on websites or their subjective evaluation of their authenticity. Other studies focusing on attributes of the recipient show that knowledge and experience with internet technology and phishing [5, 10], personal traits [5, 15] as well as demographic factors [10, 15] influence individual susceptibility to phishing attacks.

Generally, social engineering literature usually focuses on users' ability to distinguish fraudulent emails/websites from authentic ones. It is assumed that users click a link in a message or enter sensitive information in a website perceived as authentic whereas they dismiss emails/websites perceived as fraudulent.

However, according to results of previous studies [4, 6], users without specific knowledge about social engineering mostly base this distinction on properties which experts dismiss as easily fakeable (such as address, design or brand). This suggests that these "novice" users do not explicitly evaluate potential indicators of forged emails or websites as experts do, but instead apply the same indicators of trust as they do for legitimate emails and websites.

Even though both perspectives are concerned with computer-mediated interpersonal trust, currently not much cooperation between the two fields is evident and we know of no integrated approach which covers both warranted and unwarranted trust.

Integrating the Perspectives

We suggest an approach which integrates results from both the e-commerce and social engineering fields in order to understand the factors that influence trust in online communication, regardless of whether a message or website is legitimate or not.

Following this approach, we use those characteristics of the message or website (e.g. language, content, design), the sender (e.g. familiarity, reputation) and the receiver (e.g. knowledge, personality, demographics) which were found to be relevant by either of the fields to predict users' trust in an online message or website. Specifically, we are creating a model to predict a user's decision to follow or dismiss a request (such as clicking a link, providing data or opening an attachment) presented in an electronic message. A preliminary version of that model will be presented at this workshop.

The results from research following this approach will in return expand both the body of empirical evidence and the theoretical background for both fields, as each field can make use of the other field's results and theoretical considerations.

Integrating the results from both fields is possible since they actually study the same thing: Factors influencing user's trust in communication received online. Factors influencing trust which were found in experiments or interviews in social engineering studies can therefore be integrated into the trust models created and validated by e-commerce researchers in order to create a comprehensive model which predicts trust in both legitimate and fraudulent messages/websites.

Outlook

In the next step, our model will be validated empirically to test the assumption that results from both fields can be integrated in one overall model and the model will be refined according to the evaluation's results.

References

[1] Beldad, A., de Jong, M., and Steehouder, M. How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust. *Computers in Human Behavior 26*, 5 (Sept. 2010), 857–869.

[2] Britannica Online. phishing, 2012. `http://www.britannica.com/EBchecked/topic/1017431/phishing`, 2012-11-22.

[3] Corritore, C. L., Kracher, B., and Wiedenbeck, S. On-line trust: concepts, evolving themes, a model. *International Journal of Human-Computer Studies 58*, 6 (June 2003), 737–758.

[4] Dhamija, R., Tygar, J. D., and Hearst, M. Why phishing works. In *Proceedings of the SIGCHI conference on Human Factors in computing systems - CHI '06*, ACM Press (New York, New York, USA, Apr. 2006), 581.

[5] Downs, J., Holbrook, M., and Cranor, L. Behavioral Response to Phishing Risk. *Institute for Software Research 1*, 1 (2007).

[6] Downs, J. S., Holbrook, M. B., and Cranor, L. F. Decision strategies and susceptibility to phishing. In *Proceedings of the second symposium on Usable privacy and security - SOUPS '06*, ACM Press (New York, New York, USA, July 2006), 79.

[7] Goodchild, J. Social Engineering: The Basics, 2010. http://www.csoonline.com/article/514063/social- engineering-the-basics, 2012-11-22.

[8] Guha, R., Kumar, R., Raghavan, P., and Tomkins, A. Propagation of trust and distrust. In *Proceedings of the 13th conference on World Wide Web - WWW '04*, ACM Press (New York, New York, USA, May 2004), 403.

[9] Harrison McKnight, D., Choudhury, V., and Kacmar, C. The impact of initial consumer trust on intentions to transact with a web site: a trust building model. *The Journal of Strategic Information Systems 11*, 3-4 (Dec. 2002), 297–323.

[10] Jagatic, T. N., Johnson, N. A., Jakobsson, M., and Menczer, F. Social phishing. *Communications of the ACM 50*, 10 (Oct. 2007), 94–100.

[11] Karakasiliotis, A., Furnell, S., and Papadaki, M. Assessing end-user awareness of social engineering and phishing. In *Proceedings of 7th Australian Information Warfare and Security Conference* (Edith Cowan University, Perth Western Australia, 2006).

[12] Kumaraguru, P., Acquisti, A., and Cranor, L. F. Trust modelling for online transactions. In *Proceedings of the 2006 International Conference on Privacy, Security and Trust*

Bridge the Gap Between PST Technologies and Business Services - PST '06, ACM Press (New York, New York, USA, Oct. 2006), 1.

[13] Lin, E., Greenberg, S., Trotter, E., Ma, D., and Aycock, J. Does domain highlighting help people identify phishing sites? In *Proceedings of the 2011 annual conference on Human factors in computing systems - CHI '11*, ACM Press (New York, New York, USA, May 2011), 2075.

[14] McKnight, D. H., Choudhury, V., and Kacmar, C. Trust in e-commerce vendors: a two-stage model. In *ICIS '00 Proceedings of the twenty first international conference on Information systems* (Dec. 2000), 532–536.

[15] Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., and Downs, J. Who falls for phish? In *Proceedings of the 28th international conference on Human factors in computing systems - CHI '10*, ACM Press (New York, New York, USA, Apr. 2010), 373.

[16] Urban, G. L., Amyx, C., and Lorenzon, A. Online Trust: State of the Art, New Frontiers, and Research Potential. *Journal of Interactive Marketing 23*, 2 (May 2009), 179–190.

11 Improving Trust in Interactive Graphics

by Benoît Otjacques, Mickaël Stefas, and Maël Cornil

Abstract

Interactive graphics are a specific type of user interfaces for IT systems. Since they are extremely performing to convey information about data, they are intensively used for persuasive purposes. The level of trust given to an information system sometimes almost entirely relies on the reliability of the derived graphics. Studying trust in graphics appears therefore to be of utmost importance. This position paper discusses how adding appropriate visual elements can contribute to increase trust in one of the most common charts, namely the scatter plot.

Introduction

All of us have already seen some charts explaining how successful the track record of an investment is by showing a sharply rising curve. The people who really care about their money also look at the scales, the potential distortions in the graphics as well as the source of the data displayed. In the IT world, graphics are also intensively used to support tasks like network monitoring, storage system optimization or workload allocation within a team. Critical decisions are taken on the basis of such graphics. Visualization software should therefore be designed to produce graphics that are not only appealing but also trustworthy.

Two elements greatly influence the degree of trust given to graphics: the reliability of the data and the fairness of their visual representation. This paper focuses on the latter and uses the scatter plot example to point out some issues and some potential solutions.

Trust Issues in Graphics

The easiest way to modify the perception of the facts displayed in a chart is to select the appropriate subset of data that perfectly matches the message to promote. Excluding data points from a chart may result from a fully justified methodology (e.g. wrong data encoding, irrelevant outliers...), from an unconscious lack of rigor or from a deliberately unfair attitude. Traces of any exclusion should ideally be kept in order to allow a subsequent check by external actors. Building trust in graphics requires then to offer means to access the underlying data as well as to know if, how and why some data items are not displayed in the chart. For instance, following these guidelines is demanded in high quality research papers.

Presenting data in such a way that the visual result fits the message of its designer is more subtle. Rigorously speaking, nothing is wrong in the data displayed. No abusive exclusion or wrong position of points can be noted. However, the experts in visual perception know that some graphical elements take precedence on others during the cognitive process. Shapes, patterns, spatial positions or colours are not perceived in the same way and at the same speed [2]. The perception of the chart has an influence on the understanding of the underlying facts, whatever the formal correctness of the graphics. The lack of a comprehensive theory about the global perception of current advanced interactive graphics is a major issue from this perspective. Discovering the degree of honesty of the graphics designer is in fact really difficult. Therefore the level of trust given to graphics often relies on the reputation of the designer and his/her potential conflicts of interests. The graphics author should therefore be clearly identified. For instance, graphics released on their respective web site by a company selling its shares in an IPO or by the supervising authority of the financial markets do not have the same credibility. The skills of the target user of the graphics must also be taken into account. A financial analyst is probably less naive than a customer of a bank to analyse such graphics.

Trust Issues in Scatter Plots

A scatter plot basically displays the potential relationship between two variables X and Y. Typically, does the CO2 emission of a car relate to the power of its engine? The understanding of this potential X-Y relationship is clearly influenced by visual perception. For instance, a typical misuse of scatter plots consists in selecting the scale of the two axes in order to modify the perception of the reality. All data is displayed but the potential positive or negative correlation among X and Y is made abusively visible or hidden. Graphics displaying the evolution of financial markets too often use this strategy to give a false impression of stability or volatility of investment products. Similarly, adopting a non-linear scale (e.g. logarithmic scale) may be perturbing for users who do not have the appropriate education to understand it. If the scatter plot is intended to show a linear relationship between X and Y, a straight line is sometimes explicitly drawn across the data points. The relevance of this linear interpolation can be measured with statistical tests. However, the visual power of a straight line may bring the user to underestimate the results of such a test. How can we tackle these potential biases with design guidelines?

Proposals to Tackle Trust Issues

For more than five years, we have been designing and implementing a visualization tool called Calluna [1]. Among the design guidelines that have governed (and still apply to) our work, we have put much emphasis on how to avoid the user to (unconsciously) generate biased or unfair graphics. This paper points out some of our proposals aiming to improve trust in interactive scatter plots (see Figure 11.1 illustrating our suggestions).

First, it is crucial from our perspective to tell the viewer of a chart if he sees the whole dataset or only a subpart of it. How to tag the graphics with this information is left to the designer. The simplest way is probably to add a reference to an external resource

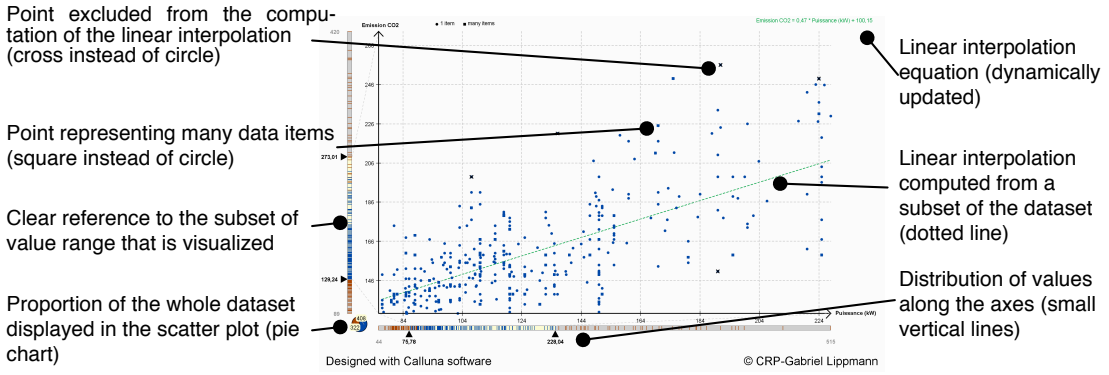

Figure 11.1. Scatter Plot with improvements to enhance trust

(e.g. web page, methodology section in a paper) that explains why some data have been excluded. We propose to go beyond this approach and to use multiple complementary visual items within the scatter plot itself to provide this information. In our tool, a small pie chart located at the origin of the axes displays which proportion of the whole dataset is currently displayed in the scatter plot. In addition, two (interactively linked) ranges of values are permanently displayed as axes of the scatter plot. The first one expands on the complete range of values encountered in the data set and the second one refers to the range of values currently displayed in the chart. Third, in many cases the X and Y values of the data items are not homogeneously distributed. Zooming on a sub- range of values may be representative of many data items or only a few. Knowing the distribution of elements according to X and Y may help in this context. They are displayed by small vertical lines on the axes. Fourth, a single point in the scatter plot may visualize one or many data items. To help the user to distinguish among these cases, distinct glyphs are used in the scatter plot (circles for points linked to one data item and squares for points linked to many data items). In addition interactive tooltips allows to know which data items a given glyph represents.

We have also studied how to support an appropriate use of linear interpolation. First, our tool allows to select data items directly in the graphics and to compute in real time the corresponding linear interpolation. By default, the complete dataset is taken into account and the interpolation equation is displayed as a continuous line. If the interpolation line refers to a subset of items, it is displayed as a dotted line (cf. Figure 11.1). For instance, an option allows to compute the equation only from the data items currently displayed in the scatter plot (cf. zoom on subset of ranges on the vertical and horizontal axes). Since the equation is permanently displayed in the upper right- hand corner of the chart, the user sees it changing as he/she modifies the selected sub-range of values on the axes. The user may also interactively exclude some specific data items from the interpolation computation. In this case, the related points are not simply removed from the scatter plot but are displayed by a cross instead of a point (cf. to keep trace of the exclusion).

Conclusions

In this paper we have drawn the attention to the fact that some graphics can be formally correct but still unfair. If static graphics can be potentially checked a posteriori by a validating authority, this approach is not possible anymore for interactive graphics produced in real time by visualization software. We argue that some visual elements can be embedded into graphics like scatter plots to facilitate the evaluation of the degree of trust that the users can give to. Generally speaking, this often means reducing the design space by setting rules preventing to create graphics known to be unfair. However, considering trust may also lead to proposals that enrich the design space with a new set of potential features and graphic components. Graphics are often used to give some feedback to the user about the behaviour or the current state of an interactive system.

Research results regarding how to improve trust in graphics may therefore also be used in tools not specifically dedicated to information visualization. It would clearly be useful to know better how the mental model of the interactive system behaviour is influenced by the graphics used to monitor this system. For instance, how is the system dynamics rendered by the graphics? More fundamentally the relationship between the levels of trust respectively given to graphics and to the interactive system that they illustrate is worth being more intensively investigated.

References

[1] Calluna Software. Calluna Software, 2012. `http://www.calluna.lu`, 2012-12-6.

[2] Ware, C. *Information Visualization: Perception for Design*. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, Apr. 2004.

12 Trust in Mobile Commerce

by Ioannis Kounelis and Jan Loeschner

Abstract

This paper describes how a citizen, in our case a user of a mobile phone, is confronted with several aspects of trust when he/she uses different mobile commercial objects in a digital world. In particular, the topic of m-commerce and how a client mitigates trust all the way from his/her mobile device to the merchant is dealt with. To assess the trust chain, especially in respect to privacy and data protection, objects (for example a voucher) are used to model the mobile commerce domain.

Introduction

Mobile communication devices, such as mobile phones, are frequently used today by almost every citizen of any age group. They are used by citizens for a big variety of activities, including personal sensitive information exchange. Therefore it is becoming common and acceptable to use them more and more for mobile commerce by executing financial transactions.

However, since monetary values are involved, this use assumes more and more trust from the client side. As defined by the Trust in Digital Life consortium [3], trust comprises the intention to accept vulnerability based on positive expectations of the intentions or behaviours of another. As a result the client lays this kind of trust to the whole technology of mobile commerce; from the hardware of the device to the mobile commerce object.

In this position paper the chain of trust in mobile commerce is described, using the paradigm of a mobile voucher. As each mobile object is handled by an application and not directly by the Operating System (O.S.), first the client's trust chain for mobile applications is described in general and later for m- commerce objects in particular.

Definitions

Below are some definitions that might be useful to know when reading this position paper.

m-commerce Mobile commerce is any transaction, involving the transfer of ownership or rights to use goods and services, which is initiated and/or completed by using mobile access to computer-mediated networks with the help of an electronic device [6].

m-objects M-objects are digital files that are used with the use of a mobile device.

voucher A voucher is a small printed piece of paper that represents the right to claim goods or services [4]. Of course in the case of an m-voucher there is no more a printed copy, but a unique identifier such as a barcode or a QR code stored locally on the phone or on the user's cloud service.

Privacy Impact Assessment (PIA) A privacy impact assessment is a methodology for assessing the impacts on privacy of a project, policy, program, service, product or other initiative which involves the processing of personal information and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimise negative impacts [7].

Common Criteria (CC) The Common Criteria for Information Technology Security Evaluation is an international standard (ISO/IEC 15408) for computer security certification [2].

Mobile Applications – Trusting the Device's Operating System's Application Market

When purchasing a mobile device, the client assumes trust on the device manufacturer that the product will perform as described. Besides the hardware, a major part of this expectation lies on the Operating System of the mobile device. Even more this trust refers to the manufacturer's way of handling personal and sensitive information while handling the device.

A few years ago the above chain was simpler since every (or almost every) manufacturer had its own Operating System. So, a user trusted one brand of mobile phones and that implied a series of other selections. Nowadays, users have more options. Choosing a mobile brand does not necessary imply the Operating System of the device. And even when selecting the Operating System, that does not mean exactly the same experiences. Especially in cases of open software (Android for example), manufacturers tend to add their own programs and controls to the native Operating System, thus creating a different experience for the user even if the core of the O.S. is the same.

As mobile applications have moved from a non-organized multisource distribution to a single centric distribution market – the application markets of the phones vendors (App store[1], Play Google[2], Windows MarketPlace[3], etc.) – the user mitigates the initial trust given to the manufacturer (and thus to the O.S.) to the download and use of the applications. So, when a user downloads an application from the market and uses it on the phone he/she trusts that this application is verified by the O.S. provider and therefore is safe and secure to use.

As a matter of fact this trust has very valid grounds: Only recently was the first infected application found on the App store [1]. On Play Google there are more cases of malicious

1. http://www.apple.com/iphone/built-in-apps/app-store.html
2. https://play.google.com/store
3. https://www.windowsphone.com/marketplace

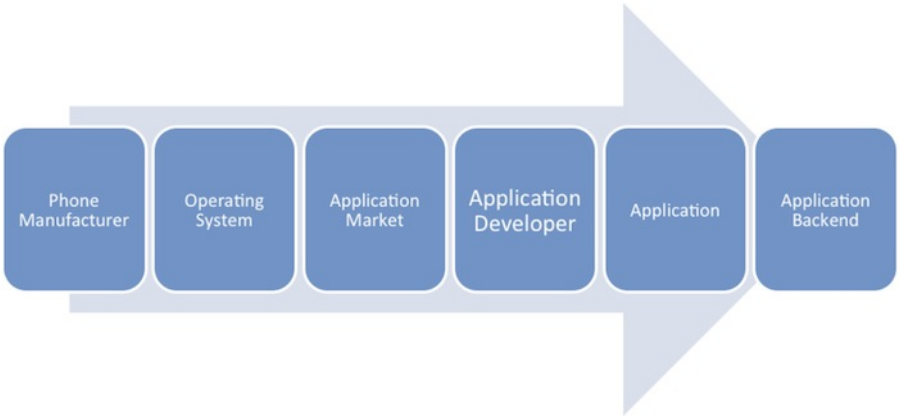

Figure 12.1. Trust chain for a client from the mobile device to the application.

applications but even in this case the applications are soon or later found and treated accordingly, even if they are already installed on the user's device. Google has introduced a malware tool called Bouncer [5] which has the role of scanning and monitoring the already approved applications on the market for malicious behavior.

However these security checks refer mostly to malware. As a result privacy violation applications are not excluded from this kind of markets. For example, an application may not contain any malware but as part of its verified process it may need to transfer some sensitive data to cloud servers, where there is no adequate security. The application itself may pass the control of the application market, but the backend security and protection of personal data cannot be checked. As the Common Criteria certification in respect to security and a PIA in respect to privacy protection are costly and resource intensive they are not carried out by the manufacturers for the mass mobile applications.

In such case how is trust mitigated, from a client point of view?

Trust has many links in the trust chain (see Figure 12.1):

- Do you trust your mobile device?
  - Hardware
  - Operating System
- Do you trust the applications that you are using on the device?
  - Application itself
  - Application Developer
  - Application Market
- Do you trust the technology behind the application (for example GSM network, SMS, Cloud storage, etc.)?

If one of the above trust bonds breaks then the whole sense of trust collapses.

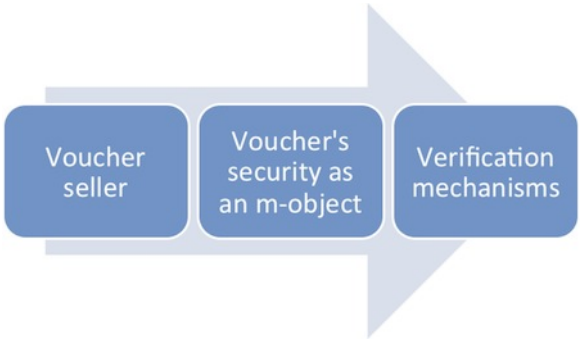

Figure 12.2. Trust chain for a voucher merchant.

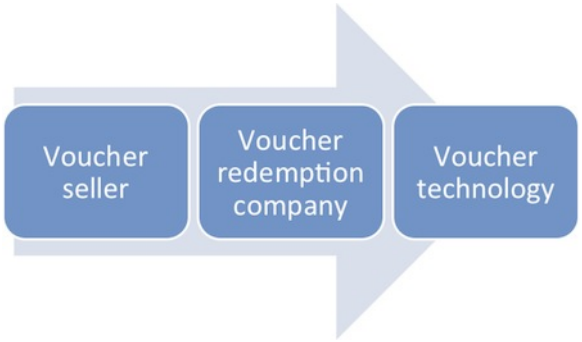

Figure 12.3. Trust chain for a voucher purchaser.

Trust Issues when delegating m-commerce objects

In this paper the paradigm of an m-voucher is used. There are three main actors in a voucher purchase: the client, the voucher seller and the voucher redeemer. Current examples of vouchers are the coupons offered by Groupon[4] or similar sites. In order to acquire a voucher an economical transaction is usually involved.

Trusting the m-commerce object is more related to verifying the authenticity and validity of the object. The same goes for tickets or any m-object that has monetary value. The importance in this case from a merchant point of view, is to trust the technology behind m-objects. Trust in the m-object entails trust in an m-object chain. For example, in the case of a m-voucher trust will be delegated to the voucher seller (which is in most cases a different company from the voucher redeemer), then trust in the m-voucher itself (ability not to be reproduced or not to be transferred to unauthorized persons, ability to reclaim/restore in case of accidental loss) and finally to the verification mechanisms (authenticity, ability to be used only as many times as it is bought for), see Figure 12.2.

From a client's point of view, the starting point of the trust chain is the same; the voucher seller. As in the case of the mobile phone manufacturer, the initial trust placed on the voucher seller company is one of great importance in order to build a successful trust bond until the end and redemption of the voucher. Second in line, after the selling company, comes the company that offers the product/service, i.e. the voucher redeemer. Even if the voucher is sold from a well-known company, if the redemption point is not trust-

4. http://www.groupon.com

worthy for the client he/she will probably avoid buying it. Finally the m-object technology is also important for the client, especially when it implies the ways of using the m-object itself (see Figure 12.3).

Conclusion

A successful m-commerce strategy needs to provide to clients the feeling of trust throughout the purchase lifecycle. If all the described trust bonds are strong so is the trust chain. As a result, if trust is guaranteed, people will be keener to use new innovative technologies that tend to replace old and traditional concepts. To prove the concept of this paper the m-objects will be model using the iCore Framework[5] to study issues like trust propagation in case of changing the owner of a m-object.

References

[1] Armando Rodriguez. Trojan Horse found in the iOS App Store: Report, 2012. `http://www.pcworld.com/article/258803/watch_out_trojan_horse_found_in_the_ios_app_store.html`, 04/12/12.

[2] Common Criteria. Common Criteria for Information Technology Security Evaluation Part 1 : Introduction and general model September 2006. Tech. Rep. September, Common Criteria, 2006.

[3] European Commission. Strategic Research Agenda: Trust in Digital Life. Tech. rep., European Commission, 2012.

[4] Fujimura, K., and Eastlake, D. Requirements and Design for Voucher Trading System (VTS). Tech. rep., RFC Editor, Mar. 2003.

[5] Kate Freeman. Google's Bouncer For Android Shows Malware Apps the Door, 2012. `http://mashable.com/2012/02/03/google-bouncer-for-android/`, 04/12/12.

[6] Tiwari, R., and Buse, S. *The Mobile Commerce Prospects: A Strategic Analysis of Opportunities in the Banking Sector*. University of Technics Hamburg, Hamburg, 2007.

[7] Wright, D., and Hert, P., Eds. *Privacy Impact Assessment*. Springer Netherlands, Dordrecht, 2012.

5. `http://www.iot-icore.eu/`