Increasing Trust Perceptions in the Internet of Things

Trenton Schulz and Ingvar Tjøstheim

Norsk Regnesentral – Norwegian Computing Center,
Gaustadalléen 23a/b, Kristen Nygaards hus, NO-0373 Oslo, Norway
{Trenton.Schulz,Ingvar.Tjostheim}@nr.no
http://www.nr.no

Abstract. When interacting with objects and services in the Internet of Things, people will need to trust that their data is safe, and that "things" will do what they promise they will do. As part of a user evaluation of a toolkit for providing security and privacy information to users, we created two models to find a pattern in changes in the perception of trust in the participants. The model based on demographics was not very descriptive. But, the model based on participants' privacy concerns and trust traits revealed a good match between changes in trust based on information from our toolkit. While there were some limitations in the current study, it showed how TFT can be improved for future evaluations.

1 Introduction

We interact with many different objects, portable, stationary or virtual, to accomplish tasks throughout the day. In the future, these objects will communicate with other objects, either locally or over the Internet. The result of this phenomenon is the *Internet of Things* (IoT) [1]. Users in the IoT will need to know that their data is protected and that their privacy is protected. This can be difficult when users are traveling in different environments and some interactions happen automatically. In short, it is desirable for users to look at privacy and security information and decide whether or not to *trust* the IoT.

Our work involves creating a Trust Feedback Toolkit (TFT) that can present information to users about the security of their connection, what data is collected, how long it is stored, and what is done with it. We have targeted smartphones and tablets for presenting this information as they are likely mobile objects that might participate in different IoT environments. We wanted to study how this information would affect users' trust of the system. Would this information make users more likely to trust or distrust a system? What sort of information makes users trust a system?

To answer these questions, we developed a user evaluation where participants interacted with several IoT environments with the aid of the TFT. We analyzed the results from the evaluations using the partial least squares (PLS) method with emphasis on the impact of the TFT. We found that for certain groups of users, the TFT did alter these users' perception of trust in the system. The impact was not always as expected, for some the effect was a decrease in trust in the system.

The contribution of this paper is to highlight a model that can find patters in changes in trust perception for users of our TFT. The paper is organized as follows. Section 2

L. Marinos and I. Askoxylakis (Eds.): HAS/HCII 2013, LNCS 8030, pp. 167–175, 2013.

provides some background and information about the terminology used in our study and how we use it; Section 3 describes how the study was carried out; Section 4 presents the results and how we created our models; Section 5 discusses these models; Finally, Section 6 provides a conclusion, lessons learned, and possible future work.

2 Background

The idea behind the IoT has been around for a while and was first used in 1999 by Ashton [1]. The IoT refers to uniquely identifiable *things*—either real or virtual—and their representation in an Internet-like infrastructure. As technology progresses, other definitions of the IoT have emerged. Here, we are looking at various things that might appear in smart environments, such as smart homes, smart offices, or e-voting. The scenarios can also be used for ambient assisted living (AAL). The things in these environments are "smart" versions of everyday objects—for example, like doors, medicine cabinets, elevators, and receptionists—and the infrastructure that is necessary for these things to work.

Trust is a concept that has many different meanings depending on the context (e.g., sociology, psychology, ethics, economics, management, and computer science). There are many reviews of trust. For example, Steinke et al. [2] take a look at trust specifically in the AAL settings. Yan et al. [3] have looked at theoretical issues when studying trust in Human-Computer Interaction. Other articles have looked at different ideas about trust in the IoT. Leister and Schulz [4] provide a summary of definitions and categories of trust while proposing an indicator for trusting a thing and its information. Even restricting the search to computer security shows differing definitions of trust [5]. There are many examples of studies that are concerned with trust perception related to the use of a particular service, for instance online banking. It is also typical to study trust at a single point in time. In contrast, Joinson and Reips [6] designed a study that looked at changes in users' trust and privacy on the Internet over a 6-week period.

While the definition of trust generated lots of discussion for us, our focus is on the user's trust. We settled on the definition presented by Döbelt et al. [7], "A user's confidence in an entity's reliability, including that user's acceptance of vulnerability in a potentially risky situation."

3 Study

The TFT has two parts: a framework for integrating into devices that catches security events and a user interface that presents information to the user and allows them to decide if they will continue with an action or not (see Fig. 1). Example information that the TFT provides is if the user is connecting to an unencrypted network, what sort of information the system wishes to store, or if a purchase will be over a certain amount. We designed an evaluation that focused on the user interface part of the TFT, and how well the information provided by the TFT aids the user in making decisions and affecting trust.

Very few have first-hand experience with the IoT. Therefore, we created two virtual reality (VR) environments to carry out user tests. One was a smart office building with

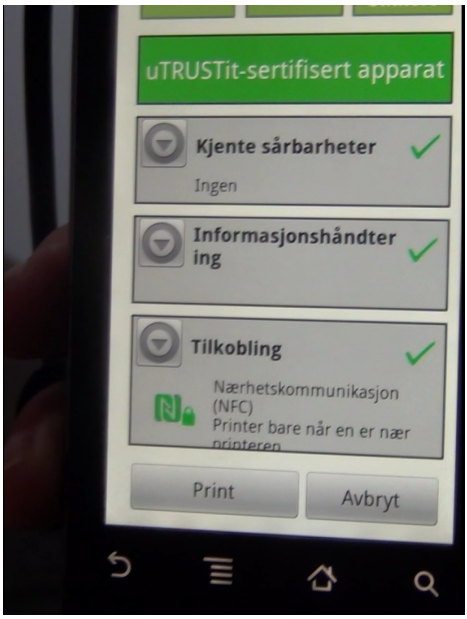

Fig. 1. An example of a TFT screen on a smartphone during the evaluations

multiple floors, meeting rooms, and break rooms. The second was a smart home environment that focused on AAL with a smart medicine cabinet that reminded users to take their medicine and door access for caregivers.

We recruited participants with different backgrounds in two different countries (Norway and Germany) to evaluate the interfaces. We followed the ethical guidelines [8] and participants filled in a consent form. Before entering the virtual environment, participants were asked to fill out questionnaires. Topics included questions about demographics (e.g., age, education level, and gender), how participants judged their own ICT abilities, their knowledge of the IoT, how they felt about certain privacy issues, and their *trust traits* [9]. The trust traits consisted of a survey where participants used a Likert scale to indicate how much they agreed or disagreed with statements about trust and security issues with the Internet, new devices, and ICT in general.

Once they had completed the questionnaires, participants were given a training session in navigation and interaction in a sample virtual environment. After participants were comfortable with the interaction (some chose not to continue), they started the evaluation in either the smart home or the smart office environment. Participants would navigate in the environment and perform tasks by interacting with the different objects using either a smartphone or a tablet. Participants were filmed during their interactions (both themselves and the screen for the smartphone or tablet), and their heart rate and skin conductivity were monitored. In total, there were 16 different tasks that the users had to perform. Four tasks were set up with the participant doing the task one time without the TFT and another time with the TFT. These tasks were: *a*) entering the break room, *b*) purchasing coffee, *c*) purchasing perfume, and *d*) ordering medicine.

After participants had completed a task, they were asked questions about their *trust state*; this consisted of four statements about trust. Participants would rate on a scale of one to four how much they agreed or disagreed with the statements (one is total disagreement, 4 is total agreement). These questions were if they felt their personal data was protected, if they trusted the security mechanisms in the system, if there was enough information about their connection to the IoT, and if they felt the network was well structured. In addition, participants needed to rate on a scale from one to four how much they trusted the things in the completed task and why. After completing all tasks, participants filled out a final questionnaire about the tasks and their experiences in virtual reality. In the end, 35 participants completed the tasks and the pre- and post-questionnaires.

After the evaluations, we created the *change in trust* variable based on four tasks that were done with and without the TFT. The variable shows a change in trust: either positive (coded as 3), no change (coded as 2), or negative (coded as 1). We designed the study to find the factors that could explain the influence of the TFT in changing trust.

4 Results

The study used a within subject design with two conditions. In condition one, the system acted without any warnings or information about the security. In condition two, the user received warnings and relevant information from the TFT regarding security. The goal was to increase trust when it is appropriate based on the information presented to the participants. Of the 35 participants, 14 felt an increase in trust in the system after using the TFT, eight felt a decrease in trust in the system, and 13 experienced no change. We will focus on those that experienced a change in trust perception.

Partial least squares (PLS) is the statistical analysis technique used to interpret data from the study and to test the two models. PLS is a structural equation modeling technique that can simultaneously estimate measurement components and structural components that are the relationships among these constructs. PLS does not require a large sample size [10, 11].

We investigated two models that could explain the influence of the TFT in changing trust. Model 1 looked at demographics—age, gender, and education—and the user's assessment of technical skills. Model 2 focused on privacy concerns and trust traits. The PLS Path Modeling for these models are shown in Fig. 2 and Fig. 3, respectively.

Model 1 showed that older people would have lower trust after seeing the information from the TFT. This was also the case for high education and high ICT skills. However, the R^2 value for this model was low (0.15) and was not very predictive. This implies that if the goal is to understand the impact of the TFT, we should look for something other than demographics.

Literature showed that privacy can be a factor that influences trust [12, 13, 14], but there is not necessarily a straightforward relationship between privacy concerns and actual behavior [6]. Another approach is to study differences caused by trust traits. We looked at both privacy and trust traits [15, 16]. We made a variable based on answers to the questions that were asked about the privacy concerns and the trust traits before participants entered the VR environment and created a new model called Model 2.

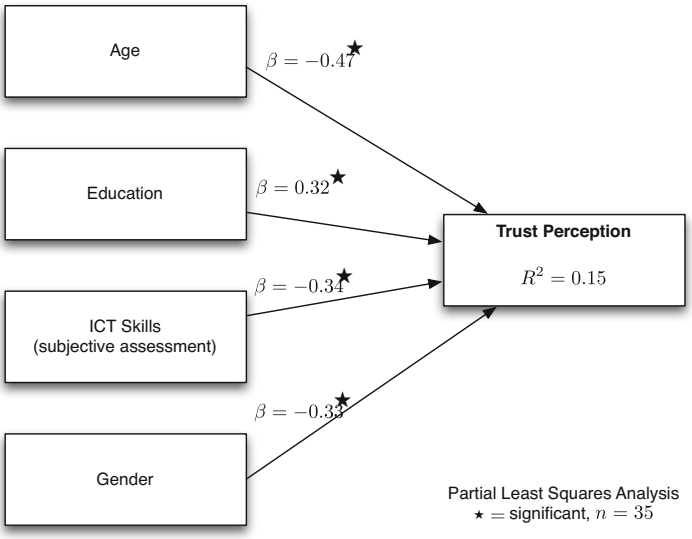

Fig. 2. Predicting change in trust perception based on demographics

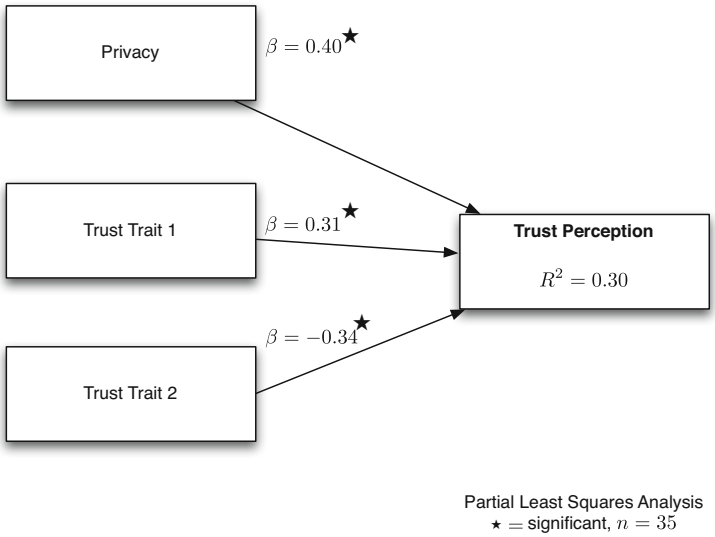

Fig. 3. Predicting change in trust perceptions based on opinions of privacy and security

Model 2 shows that the three variables show a pattern about change in the perception of trust due to information from the TFT. The participants with privacy concerns had a tendency to answer that their level of trust increased from condition one to condition two. According to this finding we can state that privacy matters. The same is true for participants that tend to be optimistic towards people, communication, and transfer of information. Yet, participants who are skeptical towards the Internet and new technology do not increase their trust when they get information from the TFT.

The R^2 value is moderate (0.30) [17]. This implies that changes in trust from the TFT are better correlated by privacy concerns and trust traits than from demographics. Table 1 shows the measurement scales for Model 2, and Table 2 shows the correlations between Model 2's latent variables.

Table 1. Summary of Measurement Scales for Model 2

Construct	Measure	Factor Loading
Privacy		
composite reliability: 0.82		
PC2	Compared to others, I am genuinely concerned about how companies and other authorities (including the Internet) process my personal data.	0.74
PC5	Compared to other topics, my private life and privacy are very important.	0.80
PC6	I am concerned about things that can threaten my private life and privacy.	0.78
Trust Trait 1		
composite reliability: 0.87		
TT7	I trust people in most circumstances.	0.83
TT8	I trust the Internet and communication.	0.90
TT9	I am normally positive about information transfer that happen through IT systems.	0.76
Trust Trait 2		
composite reliability: 0.75		
TT12	The Internet is an unsafe medium.	0.72
TT13	Generally, I feel that the Internet is an insecure environment.	0.77
TT4	I am normally careful when using new technology.	0.65

Joinson and Reips write that many people report high privacy concernts when faced with a specific threat to their privacy. In our study, the privacy factor was a significant predictor of change in trust perception. Joinson and Reips also argue that users rely "...heavily on situational cues to make a decision rather than their preexisting attitudes" [6, p.18].

Based on this, we interpret our findings as follows: both attitudinal factors—such as privacy and trust traits—matter in determining change in trust. But, a model with these factors cannot fully explain why trust increases, decreases, or does not change.

Table 2. Correlation between latent variables for Model 2

	Change in Trust Perception	Privacy	Trust Trait 1	Trust Trait 2
Change in Trust Perception	1.00			
Privacy	0.29	0.77		
Trust Trait 1	0.37	0.08	0.83	
Trust Trait 2	−0.21	0.41	0.10	0.71

Our findings also indicate that situational cues—for instance, information presented by the TFT—matter. So, the TFT is a tool that can be used to increase awareness in trust and security issues.

5 Discussion

The second structural model contains the paths between the three independent variables (constructs) and the dependent variable, the TFT. An examination of the structural model using PLS indicates that the model explains approximately 40 percent of the variability in trust perception ($R^2 = 0.30$).

According to Chin [17], R^2 values of 0.19, 0.33, and 0.67 can be described as weak, moderate, and strong, respectively. Consider also the principle of parsimony where we try to explain the most with the least. This principle favors a research model with fewer explanatory variables, assuming that this model explains the dependent variable almost as well as a model with additional variables. With the limited number of participants, it not acceptable to create many explanatory variables for a model.

In our study, the model based on demographics is weak and shows no pattern to explain trust perceptions. The model based on privacy and trust traits did show predictive power; participants having concerns about privacy and the safety of the network were influenced by the TFT and changed their perception of trust in the IoT. This helps inform designers what type of information needs to be conveyed when designing trustworthy systems for the IoT.

There are limitations with Model 2. One limitation is that it is not a comprehensive model and it has very few variables. In addition, this model is only linked to people with certain privacy concerns and trust traits. It is also difficult to say how the usability of the TFT affected the perception of trust. Usability will be included in the next evaluation.

Another limitation is the number of participants in the study. With only 35 participants it is difficult to say how our results compare to a larger sample. However, our study provides a much richer understanding of trust perception for these participants than a large questionnaire-based study. The evaluation took place in a controlled environment where the participants had context and meaningful tasks to perform. The study was designed to reveal change in trust perception because we kept other variables stable, and we measured the trust state right after completion of each task. We feel that the PLS method is helpful in showing that we get meaningful results despite a small number of participants.

Some participants reacted negatively to the TFT: they distrusted things that should have been trusted and trusted things that should have been distrusted. Sometimes, when not reflecting on what is happening, providing information may cause some participants to think there is something they need to be concerned about. In this case, suddenly getting security information—even if it shows that things are safe—when they previously received no information might cause this reaction. Ideally, the TFT should provide information so that everyone can make the right decision. Still, we see that participants with privacy concerns and certain trust traits are helped by the TFT.

Finally, skeptical users can be a difficult to serve. The findings indicate that even though we present relevant security and privacy information, skeptical users are skeptical of *that* information. It seems necessary for users to trust the TFT itself before the TFT can be play a role in informing users' trust perception.

6 Conclusion

We have created two models based on the responses that were given by participants. Model 2 gives an indication of a possible model that can be used to correlate change in trust perception. We also can see that while a survey about trust or privacy concerns can give us some information about the topic of trust, our study with virtual reality and multiple checks of the trust state allowed us to get a deeper understanding of what might cause changes in trust perception.

The evaluations provided valuable feedback on how the TFT could be improved. This resulted in a new UI for presenting security and privacy information to the user. This new UI will be tested in an upcoming evaluation in both virtual reality and the real world. The next evaluation will include more participants and focus specifically on the usability of the TFT. We expect that the next evaluation will give us a deeper understanding of what causes changes in trust perception and also lead to a better TFT that can benefit everyone.

Acknowledgments. 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 to Wolfgang Leister and Mark Summerfield for proofreading the article.

References

1. Ashton, K.: That 'Internet of Things' Thing. RFID Journal (2009), http://www.rfidjournal.com/article/view/4986
2. Steinke, F., Fritsch, T., Silbermann, L.: Trust in Ambient Assisted Living (AAL) – A Systematic Review of Trust in Automation and Assistance Systems. International Journal of Advances in Life Sciences 4(3), 77–88 (2012), http://www.iariajournals.org/life_sciences/tocv4n34.html
3. Yan, Z., Kantola, R., Zhang, P.: Theoretical Issues in the Study of Trust in Human-Computer Interaction. In: IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications, pp. 853–856. IEEE (November 2011)
4. Leister, W., Schulz, T.: Ideas for a Trust Indicator in the Internet of Things. In: Leister, W., Dini, P. (eds.) The First International Conference on Smart Systems, Devices and Technologies, SMART 2012, pp. 31–34. IARIA, Stuttgart (2012)

5. Hornák, Z., Nyilas, I., Schrammel, J., Wolkerstorfer, P., Ellensohn, L., Geven, A., Fritsch, L., Schulz, T., Abie, H., Pürzel, F., Wittstock, V.: D.3.1 Technology and Standard Report (2010), http://www.utrustit.eu/uploads/media/utrustit/uTRUSTit_D3.1_TechnologyReport_Final.pdf
6. Joinson, A., Reips, U.: Privacy, Trust, and Self-Disclosure Online. Human Computer Interaction 25(1), 1–24 (2010)
7. Döbelt, S., Busch, M., Hochleitner, C.: Defining, Understanding, Explaining TRUST within the uTRUSTit Project. Tech. rep., CURE, Vienna, Austria (2012)
8. Fuglerud, K.S., Solheim, I., Ellensohn, L., Pürzel, F., Schulz, T.: uTRUSTit Deliverable D7.4 Ethics manual. Tech. rep., Norwegian Computing Center (2011), http://www.utrustit.eu/uploads/media/utrustit/uTRUSTit_D7.4._Ethics_Manual_Final_2.0.pdf
9. Busch, M., Döbelt, S., Hochleitner, C., Wolkerstorfer, P., Schulz, T., Fuglerud, K.S., Tjøstheim, I., Pürzel, F., Wittstock, E., Dumortier, J., Vandezande, N.: uTRUSTit Deliverable D6.2. Design Iteration I: Evaluation Report. Tech. rep., CURE–Center for Usability Research and Engineering (2012), http://www.utrustit.eu/uploads/media/utrustit/uTRUSTit_D6.2-Evaluation_Report_final.pdf
10. Fornell, C., Larcker, D.F.: Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. Journal of Marketing Research 18(1), 39–50 (1981)
11. Barclay, D., Higgins, C., Thompson, R.: The Partial Least Squares (PLS) Approach to Causal Modeling: Personal Computer Adoption and Use as an Illustration. Technology Studies 2(2), 285–309 (1995)
12. Moncrieff, S., Venkatesh, S., West, G.: Dynamic privacy assessment in a smart house environment using multimodal sensing. ACM Transactions on Multimedia Computing, Communications, and Applications 5(2), 1–29 (2008)
13. Yousafzai, S.Y., Pallister, J.G., Foxall, G.R.: Strategies for building and communicating trust in electronic banking: A field experiment. Psychology and Marketing 22(2), 181–201 (2005)
14. Nixon, P., Wagealla, W., English, C., Terzis, S.: Security, Privacy and Trust Issues in Smart Environments. In: Smart Environments: Technology, Protocols and Applications, pp. 220–240. Wiley, London (2004)
15. Mooradian, T., Renzl, B., Matzler, K.: Who Trusts? Personality, Trust and Knowledge Sharing. Management Learning 37(4), 523–540 (2006)
16. Rotter, J.B.: A new scale for the measurement of interpersonal trust. Journal of Personality 35(4), 651–665 (1967)
17. Chin, W.W.: The Partial Least Squares Approach to Structural Equation Modeling. In: Modern Methods for Business Research, pp. 294–336. Laurence Wrlbaum Associates, Hillsdale (1998)