Creating Universal Designed and Trustworthy Objects for the Internet of Things

Trenton Schulz

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

Abstract. The Internet of Things promises to connect different kinds of devices, allow for new ways of interaction, and make our lives easier. But, we need to be able to trust that the Internet of Things will protect our security and privacy. It should also be universally designed so that anyone can use it regardless of ability. We applied a user-centered approach to looking at user-centered trust in the Internet of Things, including universal design issues. We conducted an evaluation with 85 participants of a security assistant that can present security and privacy information to users. The evaluation included participants who were either elderly, had vision impairment, or had dsylexia. Participants found the information useful, but there was confusion about how the UI worked. We present an updated security assistant and future areas for research in trust and the Internet of Things.

Keywords: Internet of Things, trust, universal design, usability, accessibility, security, privacy.

1 A Promising Future

As more devices gain the ability to communicate with each other, we are presented with a new idea, the Internet of Things (IoT), where objects will automatically exchange information and help make it possible to live more efficiently, collaborate more easily, and live independently for longer. The IoT gives us an opportunity for ensuring these new interaction methods and services are universally designed so the greatest amount of people benefits. Yet, these objects will be entrusted to gather data about their users and their users' habits. The IoT can also make it much easier for anyone to find out more about where we go, what we do, and who we do it with. To realize the benefit of the IoT, users need to trust that their data will be treated safely and that the objects will function correctly.

How do we create this trust? What sort of guidelines can one follow to present this information in an accessible and usable way that can be understood by as many people as possible? We have examined trust issues in the IoT with a user-centered approach, particularly in the area of smart homes, smart offices, and e-voting.

First, we examine the IoT and the definition of trust that we used during our investigation. Next, we look at a *security assistant* that can help users in presenting security and privacy information. We will also document how this information was made accessible to people with different disabilities like dyslexia and vision impairment and how

P. Zaphiris and A. Ioannou (Eds.): LCT 2014, Part II, LNCS 8524, pp. 206–214, 2014.

we evaluated the security assistant. Then, we look at the results from a user evaluation in a smart home apartment. Finally, we conclude with an updated security assistand and possible areas for future research in trust and collaboration systems.

2 The Internet of Things, User-centered Trust, and Universal Design

The *Internet of Things* (IoT) was first used by Ashton [1] in 1999 to refer to the idea of uniquely identifiable objects (things) and their virtual representations in an Internet-like structure. The idea of how the IoT will be implemented depends on the technology. For example Bassi and Horn [2] describe how RFID technology can be used to create an IoT for tracking objects, and Vermesan, Harrison, Vogt, Kalaboukas, Wouters, Gusmeroli, and Haller [3] presents the argument of the IoT being an integral part of the future Internet, with things being involved in everything from the power grid to your clothing. We went with the latter definition as it gave us a broader base for potential users to understand the implications of the IoT.

Trust is another term that has different meanings in different disciplines. In our investigations, the two disciplines where we had the most conflict, was between computer science and social sciences. In information security, Quirin, Fritsch, Husseiki, and Samson [4] point out that the ITU-T X.509 standard defines trust as an entity functioning the way it is expected to. Further, Quirin et al. state trust in information security is always, "... the correct function of a technical component that is important for the system security." From a user's perspective, this manifests itself in the authenticity of hardware or a service and usually involves some sort of certification or public key infrastructure. This means looking at the areas of online transactions and banking [5, 6]. In other areas of computer science, Yan, Kantola, and Zhang [7] try to lay out a theoretical approach for describing trust in human-computer interaction.

In social sciences, a focus area is interpersonal trust, which is not only about the expectation that things will do what they claim, but also the risk involved for the person required to trust (*trustor*). Mooradian, Renzl, and Matzler [8] examine how personality can affect the willingness to trust someone and share knowledge. Bansal, Zahedi, and Gefen [9] discuss how an individual's perception of risk in providing health information online can affect the success of a healthcare websites.

Since we were working in a cross-discplinary investigation, we struggled to find a definition of trust that could be accepted by the different disciplines. After much discussion, we settled on the definition presented by Döbelt, Busch, and Hochleitner [10, p. 23], "A user's confidence in an entity's reliability, including user's acceptance of vulnerability in a potentially risky situation." The focus on the user being willing to take the risk and use an object emphasized our focus on user-centered trust, but we still highlighted the technical component from computer science that the other entity should function as advertised. Döbelt et al. try to make a distinction between trust and *trustworthiness*. A user trusts something, but an object does not trust; it is instead trustworthy if it is trusted by the user.

The concept of *universal design* was introduced in the mid-1980s by the architect Ronald Mace, and has since then been adopted in many fields, including the design of

ICT [11]. Many think of universal design as design for people with disabilities. Yet, the general intention of universal design in ICT is to design an object so that it can be used by as many people as possible, i.e., mainstream technology for everyone, including the elderly and people with disabilities. The emphasis is on avoiding unnecessary special solutions and to provide equality and equal opportunities to participate in the society [12]. For ICT, this normally means adding bits of semantic information so it is *accessible* via assistive technology (AT) without extra set up.

Finally, the concept of universal design has two aspects: a process and a result. That is, universal design denotes (*a*) a design process or an approach and (*b*) a design that can be used by as many people as possible.

3 User Evaluations

In the past, we have examined how users perceive trust in the IoT by designing a model [13] and in virtual reality environments [14, 15]. This work was combined with a study on presenting trust information and resulted in a set of guidelines [16] for an interface for presenting trust information (Fig. 1) called the *security assistant*. The security assistant is divided into multiple layers. Layer 1 is a high-level assessment of the situation coded into four different levels: 1 (lowest) to 4 (highest). The security level is also conveyed by using colors. Layer 2 provides a simplified explanation of the levels along with a recommendation if the user should proceed or not. Layer 3 is targeted at users desiring more information about what factors and state have determined the security level. Layer 4 is for users that are curious about different terms in information security and want to find out their meaning. The idea is to provide users with the security level at a glance, but allow users to check the resulting layers to find out why this security level was chosen to build their trust in the security assistant.

After the general layout of the security assistant had been decided, we began looking at ways to make it more accessible, especially to AT. We made sure that no essential information was conveyed by one only modality. For example, the colors are used as an aid to display the security level, but this information is also presented as numbers that can be read and interpreted by AT. However, the security level number needs to be presented to the AT in a usable way. While a sighted user has the position and highlighting to see the indicated security level, this context is not sent to AT by default. Instead, an AT like a screen reader only says "1. 2. 3. 4." We added context so that the security level instead read, "Security Level 4 of 4, Excellent Security." This matches the intent of what the graphics are showing.

Normally, people in the IoT are interested in accomplishing some task and security and privacy are only a secondary goal. We wanted to make sure that the security assistant's information was understandable to as many people as possible. Graf et al. [16] found that the term "security" was most understandable term when discussing privacy, security, and trust issues with the potential users. In addition, we went through the text presented in the Layer 2 recommendation so that it was easy to understand for the majority of users, and we worked to reduce the amount the text so that people with dyslexia could easily read it.

We wanted to test the security assistant in a variety of environments and decided to perform the evaluations in a smart home, smart office, and e-voting environment.

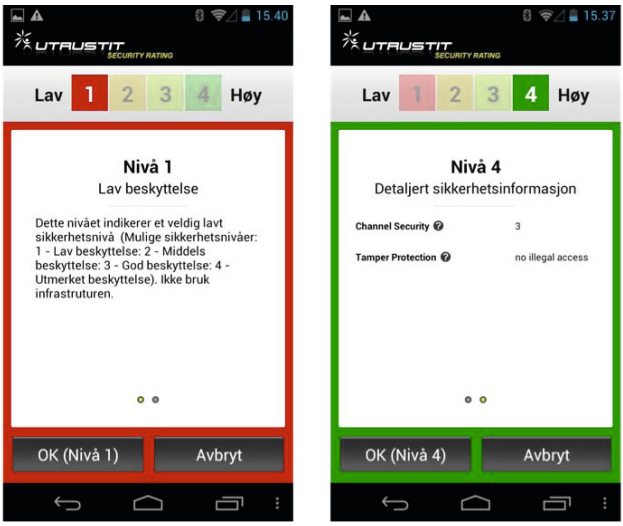

Fig. 1. The security assistant showing the first two layers of security information (*left*) and the detailed information (*right*)

So, we needed to make these environments and prototypes accessible for people with disabilities. We went through the different mobile applications and devices that were under development and made adjustments as was done with the security assistant itself. To help ensure that things worked with accessible technology, an accessibility expert worked with the developers at a two-day workshop where everyone worked with the prototypes and AT to find deficiencies.

We performed a user evaluation of the security assistant with 85 participants in Germany, Austria, and Norway. The tests in Germany used a virtual reality setting where users navigated the environment using a Kinect. The tests in Austria used a laboratory environment, and the tests in Norway were conducted in a smart home apartment.

Before beginning the evaluation, participants were surveyed about their general feelings about technology, trust, and privacy. Then, participants performed nine different tasks in the smart home and smart office environments using a phone or tablet and other objects in the environment depending on the task. Half of the participants received a low security environment and half received the high security environment. As they performed each task, participants were asked to evaluate their opinion of trust, both in the environment and in what was presented by the security assistant. Participants were then asked to provide their overall opinion of the security assistant. Finally, in Austria and Norway, participants finished the evaluation by participating in an e-voting scenario for a housing cooperative.

We evaluated 23 participants in Norway (Fig. 2). The participants consisted of five visually impaired using TalkBack (Android's screen reader application), seven visually impaired depending on text enlargement (either via software or a magnifying class) and good contrast, five with reading and writing difficulties, and six elderly.

Fig. 2. A participant testing out the medicine cabinet in the bedroom of the smart home apartment in Norway; *photo source: Aftenposten/Robert McPherson* [17]

After the evaluations were completed, the answers to the surveys were compiled to understand participants' opinions on trust in the different situations and their opinions on the security assistant. For looking at accessibility, we entered the notes from each user session into a digital system. These notes included observed behavior and comments from the participants. We used an open-code process, often used during the first steps of a qualitative analysis as described by Crang and Cook [18, p. 137] to group these observation and comments into different themes. These themes were then used as the basis for determining the accessibility of the security assistant.

4 Participants' Feelings on Trust and Accessibility

This is a summary of the participants opinions on using the security assistant and their experiences with the accessibility features. Detailed findings information for trust and universal design is provided in a separate report report [19].

Participants generally accepted the advice that they were given during the tasks, regardless of whether or not they are in a high security or low security environment. Most of the participants only looked at the first two layers of the security assistant (the security level and recommendation); few bothered to look at the details in Layer 3. One of the reasons for this could be that participants had to swipe the screen to the left to get access to the third and fourth layers. The hint that more information was available via this gesture was not obvious and few users recognized this.

Trusting the security assistant was an issue for some participants. They would ask, "where does the security assistant get this information?" and "how does the security assistant know this?" This indicates that even if the information provided by the security assistant is accurate, a user needs to trust the source of the information and its messenger.

Some participants misunderstood how the security assistant worked. The security assistant reports on security, but some participants would tap on the security level to

change it. Changing the security level was *not* intended (and didn't work), but it could be that the user interface for showing the security level (Fig. 1) may have been mistaken for buttons. None of the participants that used TalkBack to access the security assistant had this problem. This indicates TalkBack gave enough contextual information.

After it was understood that they could not change the security level from the security assistant, they were able to complete tasks. Most participants understood the concept of the security assistant, but felt they needed help to learn how it worked. The assistant helped some to realize the flow of information and how much implicit trust they were giving the objects around them. Others complained about being interrupted by the security assistant during the different tasks. Since we were evaluating the security assistant, it was necessary to be interrupted, though some participants tapped through for the final tasks.

Almost all participants with disabilities were able to complete the tasks in the evaluations and were able to get the information from the security assistant. Testing in the real world environment revealed issues with contrast and text size that we didn't not discover during development. Even though we attempted to use good color contrast and a large text size, the resolution of a screen, its color gamut, and glare due to its position in the environment resulted in less contrast and smaller text than we expected. Part of this could have been prevented by getting a higher quality display and making sure that text is a minimum physical size (i.e., measuring the size in millimeters not points or pixels), but sometimes the screen needs to be tested in the environment it's intended for to see how well it works.

Participants using TalkBack had problems using was the medicine cabinet. The medicine cabinet had a built-in screen that used its own version of TalkBack. However, this version of TalkBack was different than the one on the phones and tablets. It couldn't be upgraded and used a much different metaphor for interaction that made it difficult to use; participants using TalkBack had to give up and move on.

There were also some differences in using TalkBack between the phone and tablet that were used during the evaluation, but this did not stop the participants from completing the tasks. However, we found that the order of the information could have been presented in a more optimal way. First, TalkBack reads the security level (Layer 1). Then, TalkBack would read information about the security level and the recommendation (Layer 2) before going to the buttons to continue or cancel the action. This matches the visual layout of the security assistant (Fig. 1), but it did not match how many non-TalkBack participants used the security assistant; most looked at the security level and then pushed one of the buttons at the bottom of the screen. It probably would have been better for TalkBack to read buttons after the security level, curious users could then be informed that additional information was available.

5 Summary and Future Work

Overall, there are some issues with the security assistant, but the evaluation shows that the security assistant is a tool that can present privacy, security, and trust information in different situations to a varied group of users. In addition, the focus on universal design made it possible to uncover deeper accessibility issues due to placement or set up of information and highlights the value of real world testing by people with disabilities.

We used the information from the evaluation to improve the design of the security assistant (Fig. 3). For example, we changed the design of the security level indicator to make it more obvious that it is presenting information and not a control for changing the security level. Besides the swipe gesture, we have also added a button to make it more obvious that information in Layers 3 and 4 can be accessed. This will help determine if users need the progressive disclosure of information or are satisfied with only the first two layers. We also made the *Cancel* and *Accept* buttons change size depending on what the assistant recommended. For example, the *Cancel* button would take more space if the assistant felt one should not continue.

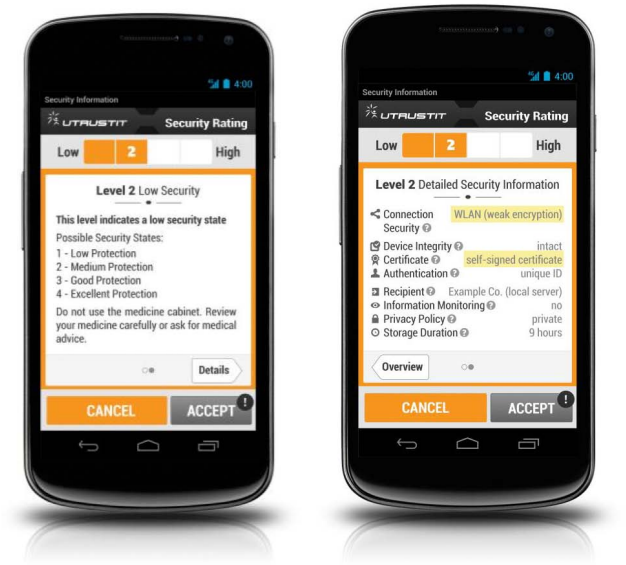

Fig. 3. The updated security assistant

For future research, work needs to be done to indicate that people can trust the security assistant. Our evaluation showed that sometimes the security assistant got in the way. How and when should the security assistant show its info? Also, the IoT has the potential to be ubiquitous, and we may not always have a device like a smartphone with us; what other methods and objects might be effective for conveying the security and trust information?

We created a set of guidelines [20] for creating new interfaces in the IoT. The guidelines provide principles based on usability heuristics and experience from past usability projects, and they detail how we created the final version of the security assistant. There is also information about designing accessible applications for Android mobile devices and how to include universal design throughout a project. The document is written to be applicable in areas outside the IoT.

User-centered trust and universal design can be applicable in other areas. For example, collaborative and learning environments need users to exchanging information and determine what they should do with it. Yet, the environment still needs to respect users' security and privacy, and it should be possible to use it regardless of ability. Everyone can benefit from having a safe environment for exchanging ideas and working together.

Acknowledgments. This research was funded as part of the uTRUSTit project. The uTRUSTit project is funded by the EU FP7 program (Grant agreement no: 258360). Thanks to Mark Summerfield and Wolfgang Leister for proofreading the article.

References

1. Ashton, K.: That 'Internet of Things' Thing. RFID Journal (2009), http://www.rfidjournal.com/article/view/4986
2. Bassi, A., Horn, G.: Internet of Things in 2020: A Roadmap for the Future (2008)
3. Vermesan, O., Harrison, M., Vogt, H., Kalaboukas, K., Wouters, K., Gusmeroli, S., Haller, S.: Internet of Things Strategic Research Agenda. In: Sundmaeker, H., Guillemin, P., Friess, P., Woelfflé, S. (eds.) Vision and Challenges for Realising the Internet of Things, ch. 3, pp. 39–82. Publications Office of the European Union, Luxembourg (2010)
4. Quirin, T., Fritsch, L., Husseiki, R., Samson, F.: Ergänzende und alternative Techniken zu Trusted Computing. Tech. rep., Sirrix AG security technologies, Bochum (2010)
5. Wang, H.: Review of studies on online consumer trust. In: Second International Conference on Computational Intelligence and Natural Computing, pp. 97–100. IEEE (September 2010)
6. Law, K.: Impact of Perceived Security on Consumer Trust in Online Banking. Master, AUT University, Auckland, New Zealand (2007)
7. 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)
8. Mooradian, T., Renzl, B., Matzler, K.: Who Trusts? Personality, Trust and Knowledge Sharing. Management Learning 37(4), 523–540 (2006)
9. Bansal, G., Zahedi, F., Gefen, D.: The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. Decision Support Systems 49(2), 138–150 (2010)
10. Döbelt, S., Busch, M., Hochleitner, C.: Defining, Understanding, Explaining TRUST within the uTRUSTit Project. Tech. rep., CURE, Vienna, Austria (2012)
11. The Center for Universal Design: About UD (2008), http://www.ncsu.edu/ncsu/design/cud/about_ud/about_ud.htm
12. Aslaksen, F., Bergh, S., Bringa, O.R., Heggem, E.K.: Universal Design: Planning and Design for All (1997), http://home.online.no/~bringa/universal.htm
13. Leister, W., Schulz, T.: Ideas for a Trust Indicator in the Internet of Things. In: Leister, W., Dini, P. (eds.) SMART 2012—The First International Conference on Smart Systems, Devices and Technologies, No. c, pp. 31–34. IARIA, Stuttgart (2012)
14. Schulz, T., Tjøstheim, I.: Increasing Trust Perceptions in the Internet of Things. In: Marinos, L., Askoxylakis, I. (eds.) HAS/HCII 2013. LNCS, vol. 8030, pp. 167–175. Springer, Heidelberg (2013)
15. Busch, M., Hochleitner, C., Lorenz, M., Schulz, T., Tscheligi, M., Wittstock, E.: All In: Targeting Trustworthiness for Special Needs User Groups in the Internet of Things. In: Huth, M., Asokan, N., Čapkun, S., Flechais, I., Coles-Kemp, L. (eds.) TRUST 2013. LNCS, vol. 7904, pp. 223–231. Springer, Heidelberg (2013)

16. Graf, C., Busch, M., Schulz, T., Hochleitner, C., Fuglerud, K.S.: D.2.7 Updated Design Guidelines on the Security Feedback Provided by the "Things". Tech. rep., CURE, Vienna, Austria (2012)
17. Hexeberg, A., McPherson, R., Færaas, A.: Ville du bodd i et hus hvor alt er koblet til Internett? (May 2013), http://www.aftenposten.no/nyheter/iriks/Ville-du-bodd-i-et-hus-hvor-alt-er-koblet-til-Internett-7192204.html
18. Crang, M., Cook, I.: Doing Ethnographies. Sage Publications Ltd., Los Angeles (2007)
19. Busch, M., Wolkerstorfer, P., Hochleitner, C., Schulz, T., Fuglerud, K.S., Tjøstheim, I., Leister, W., Solheim, I., Lorenz, M., Wittstock, E., Dumortier, J., Vandezande, N., Petro, D.: D6.3 Design Iteration II – Evaluation Report. Tech. rep., CURE, Vienna, Austria (2013)
20. Klein, M., Wolkerstorfer, P., Hochleitner, C., Fuglerud, K.S., Schulz, T.: D2.8 Final UI-Guidelines for the Trust Feedback Provided by the IoT. Tech. rep., CURE, Vienna, Austria (2013)