Privacy, Trust and Interaction in the Internet of Things

Johann Schrammel[1], Christina Hochleitner[1], and Manfred Tscheligi[1,2]

[1] CURE, Center for Usability Research & Engineering
Modecenterstraße 17 / Objekt 2, 1110 Wien, Austria
[2] HCI Unit, ICT&S, University of Salzburg
Sigmund-Haffner-Gasse 18, 5020 Salzburg, Austria
{schrammel,hochleitner,tscheligi}@cure.at

Abstract. This workshop addresses topics of increasing importance in the emerging area of the Internet of Things (IoT): privacy, trust and related interaction concepts. The aim of the workshop is to bring together experts from different areas to cover the complexity of the questions involved and to provide a forum for developing new ideas on how to address the major challenges in the field considering both a scientific and an industrial viewpoint. The workshop targets to identify pressing questions and to develop a research agenda for trusted and privacy-respecting computing in the IoT. Special attention within the workshop is given on whether and how experiences with privacy and trust from related areas can be applied to the IoT, where existing conceptualizations need to be extended or modified and where radically new concepts are required.

The Internet of Things (IoT) is an umbrella term covering a number of different base technologies aimed at linking physical objects and their virtual representation with the goal to utilize this link for improved service and interaction concepts [3]. The IoT approach combines concepts and paradigms informed by Ambient Intelligence, Ubiquitous Computing, Sensor Networks, Grid Computing, etc. Even though the IoT is still a vision and far from being a reality, more and more aspects of it become already tangible. For example, objects are equipped on large scale with RFID-tags for logistics purposes, formerly stand-alone devices become connected to the net and the "smart home" knows where a user left his glasses.

Looking a little closer into potential effects and implications of such scenarios it becomes immediately evident that there are serious privacy, trust and related interaction issues that need to be addressed to allow taking full advantage of the potentials of the IoT. For example, being able to find a specific book within your library at once is a nice feature. However, providing others the possibility to know, analyze and interpret when you were reading which book might be far less desirable.

Privacy issues have been researched in many related areas e.g. [3][4][5]. In the IoT however new sets of potentially sensitive data becomes available through profiling of "things", and questions regarding what this data is telling about the user and who should be allowed to see and use this information have to be raised. The key issue is “how one is being read (and interpreted in a possibly mismatching context) by someone else” [4]. Another new dimension of privacy aspects in the internet of things is the vast amount of objects and data that has to be dealt with. Whereas the related ubicomp scenarios typically only deal with selected subsets of actions and dedicated

D. Keyson et al. (Eds.): AmI 2011, LNCS 7040, pp. 378–379, 2011.

devices in the IoT literally everything in the users environment needs to be considered with regard to privacy aspects. Due to the amount and hiddenness of information new dimensions of complexity in the formulation of privacy concepts, the engineering of privacy policies, and the management of information privacy emerge. Research has shown that the information on social networking sites has the potential for severe consequences, and that users have difficulties to correctly understand possible long-term effects of their behavior [1]. Even more severe problems have to be expected for a wide-scale application of IoT-concepts.

Closely related to these privacy issues is the question on how a basic level of trust can be supported and achieved within the IoT. Little is known on how models of trust that are formed both in interaction in human society and in the context of desktop computing can be transformed towards the IoT, which specific difficulties, misconceptions and challenges might arise, and how they can be accounted for from a design perspective. Currently, trust is often anchored in a strictly technological context, which is easily misinterpreted by humans and miscommunicated by system vendors and owners. Therefore we want to further develop the understanding of relevant factors for the perception and formation of trust in the context of the IoT.

Another specifically challenging aspect of the IoT is that only very limited feedback and interaction possibilities are available to communicate the current status of the system and the data exchange. Due to the pervasive and ubiquitous nature of the everyday objects they only can be enhanced with little information bits, thereby making it extremely challenging to communicate complex patterns of data transmission and privacy status. The typical communication bandwidth of an object within the IoT might be one bit: on or off, possibly displayed by use of a LED or similar means. Here the question is how much (status) information regarding privacy issues can be communicated with such restricted possibilities, and what other means to keep user informed and aware of what's going on can be utilized in the IoT context.

In detail the workshop addresses the following questions and objectives: What are the main (new) privacy challenges arising from the IoT-concept? How do existing solutions for privacy scale within the IoT? What are the mental models of trust that users form with regard to the IoT? Which metaphors can be used to support users in developing helpful and reality-conform mental models in IoT-settings? Which (simple) interaction mechanisms and concepts are suited best for providing feedback in the IoT? What supporting measures and mechanisms are available to help users to form a proper understanding of the IoT?

References

1. Acquisti, A., Grossklags, J.: Privacy Attitudes and Privacy Behaviour. In: Camp, J., Lewis, R. (eds.) Economics of Information Security, pp. 165–178. Springer, NY (2004)
2. Fritsch, L.: Profiling and Location-Based Services. In: Hildebrandt, M., Gutwirth, S. (eds.) Profiling the European Citizen, pp. 147–160. Springer, Netherlands (2008)
3. Gershenfeld, N., Krikorian, R., Cohen, D.: The Internet of Things. Scientific American 291, 76–81 (2004)
4. Hildebrandt, M.: An Ecosystem of Legal and Technological Protections, on: Trusted e-services for the citizen session. In: ICT Event 2010, Brussels (2010)
5. Langheinrich, M.: Privacy in Ubiquitous Computing. In: Krumm, J. (ed.) Ubiquitous Computing. Chapman & Hall / CRC Press (2009)