Supporting Transparency and Privacy in Emerging IoT Environments

Peter Shaw[1], Mateusz Mikusz[1], Nigel Davies[1], Sarah Clinch[2] and Christoph Dibak[3]
[1]Lancaster University, [2]University of Manchester, [3]University of Stuttgart

Rapid advances in low-cost sensing, actuation and communication technologies are leading to the widespread deployment of IoT devices in a range of physical spaces, ranging from private domestic dwellings through to public and semi-public spaces, such as transport hubs, city streets, municipal parks, cafes, hotels, office complexes and meeting rooms. These IoT sensing devices and infrastructures can support a wealth of new services including the provisioning of statistics on space usage, detailed insights into the identity, demographics and behaviour of individuals present in the space and enabling the personalisation of shared spaces including workplaces. However, much of the IoT technology that is being deployed is deliberately designed to be an ambient (invisible) feature of the environment — the technology does not communicate its presence, purpose, practice and analysis to the wider audience it is monitoring. The result is that users of physical spaces are increasingly unaware of the technology that is being used for data capture in the spaces they inhabit, nor are they aware of how such data is exploited to provide new insights, actionable outputs and services that directly affect their lives. Providing insights and control over about data collection and use within the context of the IoT is of growing importance, in particular due to the differing levels of privacy awareness and concern among users [1]. In response to the challenges raised, researchers have proposed new approaches to providing users with appropriate control over the sensitive data gathered about them by IoT sensors. In particular, recent research has suggested the use of *privacy mediators* [2, 3] to process privacy-compromising sensor streams prior to their use by third parties.

In this presentation we will describe the design and implementation of an enhanced privacy mediator approach to privacy protection in IoT-rich environments combining mobile technology and Cloudlets. The approach provides users with both *awareness* of deployed IoT devices and a mechanism for *controlling* the data devices' capture. A distinguishing feature of our work is a focus on location rather than proximity for detecting privacy issues. Most existing approaches to awareness and interaction with pervasive environments rely on short-range communications to validate user proximity. However, research has shown that this approach is fundamentally flawed as it conflates two distinct issues - the physical area in which a user wants to interact with a pervasive environment and the propagation associated with a given wireless technology [4]. We discard proximity solutions in favour of using location data to provide maps that users can interrogate ahead of time to understand the data capture landscape as they navigate pervasive environments. Our implementation is being evaluated in a prototype smart environment that provides users with awareness and control over their privacy.

[1] P. Porambage, M. Ylianttila, C. Schmitt, P. Kumar, A. Gurtov, and A. V. Vasilakos, "The quest for privacy in the internet of things,"*IEEE Cloud Computing*, vol. 3, no. 2, pp. 36–45, Mar 2016.

[2] U.S. Federal Trade Commission, "Internet of things – privacy & security in a connected world," Department of Computer Science, Michigan State University, Tech. Rep., January 2015.

[3] N. Davies, N. Taft, M. Satyanarayanan, S. Clinch, and B. Amos, "Privacy mediators: Helping iot cross the chasm," in *Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications*, ser. HotMobile '16. New York, NY, USA: ACM, 2016, pp. 39–44. [Online]. Available: http://doi.acm.org/10.1145/2873587.2873600.

[4] N. Davies, M. Langheinrich, S. Clinch, I. Elhart, A. Friday, T. Ku- bitza, and B. Surajbali, "Personalisation and privacy in future pervasive display networks," in *Proceedings of the 32nd annual ACM conference on Human factors in computing systems*. ACM, 2014, pp. 2357–2366.

This research is partially funded through the EPSRC under grants EP/N028228/1 (PACTMAN:Trust, Privacy and Consent in Future Pervasive Environments) and “PETRAS IoT Research Hub – Cybersecurity of the Internet of Things” (EP/N023234/1).