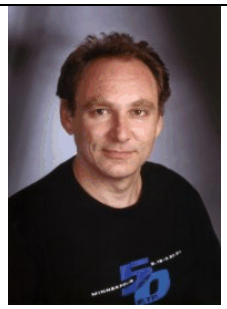
Guest Editorial

				
Richard Mortier	Jon Crowcroft	Charith Perera	Sasu Tarkoma	Peter Christen

Privacy Issues in Internet of Things

The long-heralded Internet of Things is finally becoming a reality. From factories and the ubiquitous Internet-connected fridge, we now see heating control systems, cars, dishwashers and all manner of common-place devices being connected. While this has certainly realised new capabilities, such as the ability to control one's domestic heating remotely, the benefits are perhaps more mixed: every device that we can remotely control is a device that someone else can remotely hack. And that is just the devices – the literal things; in tandem we also see increasing intrusion of Internet-connectivity into services, practices and everyday infrastructures such as transport and retail. Coupled with the increasingly invasive deployment of these devices into everyday lives, the result is a substantial increase in threats to privacy arising from the Internet of Things.

We thus felt that Privacy Issues in the Internet of Things was a topic ripe for exploration and a Special Issue in this journal. We received a strong response to the Call, with submissions from around the world: Europe, Asia, India, Russia, America. We were also pleased to see that submissions came from both academic and industrial researchers, in some cases in collaboration. Following a rigorous review process – each paper received two expert reviews, as well as being reviewed by at least one guest editor – we were able to accept four submissions, which we now introduce.

We begin with two papers related to security of the Internet of Things. The first, "A Lightweight Biometrics based Remote User Authentication for IoT Services" addresses the problem of how IoT devices can ensure that they are communicating with the appropriate party. The authors present a scheme for mutual authentication between resource-constrained devices, using a combination of user password and biometric data. Their scheme follows up mutual authentication by agreeing session keys with which to encrypt subsequent communication.

The second, "Facilitating the Delegation of Use for Private Devices in the Era of the Internet of Wearable Things", focuses on the particular class of IoT devices that are wearable, and offer great possibilities for customisation as a result. The authors note that the constraints these devices impose – even more highly restricted power and intermittent connectivity than other IoT devices – makes it difficult to apply standard techniques for maintaining "data security, integrity and reliability". Within this scope, the authors consider the specific problem of how the owner of a wearable IoT device may securely delegate use of the device for a limited period of time. They present six related protocols: the first and last associate and

de-associate the device to a cloud service, while the other four provide for delegation and reclamation of the device under both reliable and unreliable connectivity conditions.

The remaining two papers focus on privacy preservation in two quite different domains. The first of these, "Privacy-Preserving Mechanisms for Crowdsensing: Survey and Research Challenges", examines the particular challenge of privacy preservation in crowdsensing, where the many and varied sensors in users' (mobile) devices are used to sense and report on their situation and the environment around them. The authors first describe the domain in general terms, followed by a focus on specific design considerations identified for privacy-preservation. They then present a taxonomy of current mechanisms structured around the two major processes in which participants are involved: *tasking*, where mobile devices are given instructions as to what to collect; and *reporting*, where the devices actually report sensed data, typically to a cloud service. They finish with a discussion of open challenges in this area.

Finally, "Privacy-Preserving Power Injection over a Hybrid AMI/LTE Smart Grid Network", takes a view of the Internet of Things at a different scale, focusing on the increasingly widely deployed ability of consumers to inject excess power generated from (e.g.,) renewable energy sources, back into the so-called Smart Grid. The authors address the tension between the need to create a fair market in which consumers can sell energy back to the grid, and the desire for those consumers to retain privacy particularly concerning the amount of energy they have stored. Assuming the presence of both an "Advanced Metering Infrastructure (AMI)" and modern cellular networks (the so-called "Long-Term Evolution (LTE)" network), they present and evaluate in simulation a scheme that achieves two goals. Consumer bids for sale are aggregated to prevent an individual bid from being determined by the utility company, while retaining the ability for the utility company to ensure the integrity and authenticity of that aggregate bid.

To conclude, we would like to thank all the authors who submitted work to this issue and who worked with us on revisions; all the external reviewers on whose expertise we relied; and, of course, the journal's staff in producing this Special Issue. We hope you enjoy it!

BIOGRAPHIES

- Richard Mortier

Richard Mortier is a University Lecturer in the Cambridge University Computer Laboratory's Systems Research Group. He has previously worked for Microsoft Research and Sprint Labs, as well as for startups including Cplane Inc., Vipadia Limited, and currently works with Docker Inc. He holds a Ph.D. in Computer Science from the University of Cambridge following graduation in Mathematics and receipt of the Diploma in Computer Science, also from Cambridge University. Past work includes Internet routing, distributed system performance analysis, network management, aesthetic designable machine-readable codes and home networking. He works in the intersection of systems with HCI, building user-centric systems infrastructure to enable Human-Data Interaction in our ubiquitous computing world. For more, see http://mort.io/.

- Jon Crowcroft

Jon Crowcroft has been the Marconi Professor of Communications Systems in the Computer Laboratory since October 2001. He has worked in the area of Internet support for multimedia

communications for over 30 years. Three main topics of interest have been scalable multicast routing, practical approaches to traffic management, and the design of deployable end-to-end protocols. Current active research areas are Opportunistic Communications, Social Networks, and techniques and algorithms to scale infrastructure-free mobile systems. He leans towards a "build and learn" paradigm for research. He graduated in Physics from Trinity College, University of Cambridge in 1979, gained an MSc in Computing in 1981 and PhD in 1993, both from UCL. He is a Fellow the Royal Society, a Fellow of the ACM, a Fellow of the British Computer Society, a Fellow of the IET and the Royal Academy of Engineering and a Fellow of the IEEE. He likes teaching, and has published a few books based on learning materials.

- Charith Perera

Charith Perera holds a PhD in Computer Science from The Australian National University, Canberra, Australia and a BSc (Hons) in Computer Science from Staffordshire University, Stoke-on-Trent, United Kingdom. He specialized in building Internet of Things and Sensing as a Service platforms focusing on privacy aspects. His research interests are Internet of Things, Sensing as a Service, Privacy, Middleware Platforms, Distributed Sensing and Analytics Infrastructure. From 2015-2017, he worked at the Open University, United Kingdom as a post-doctoral Researcher. Previously, from 2011-2015, he worked at Information Engineering Laboratory, ICT Centre, CSIRO as a doctoral trainee. He is a member of both IEEE and ACM.

- Sasu Tarkoma

Sasu Tarkoma is a Professor of Computer Science at the University of Helsinki, and Head of the Department of Computer Science. He is also affiliated with the Helsinki Institute for Information Technology HIIT. He has authored 4 textbooks and has published over 160 scientific articles. His research interests are Internet technology, distributed systems, and mobile and ubiquitous computing. He has seven granted US Patents. His research has received several Best Paper awards and mentions, for example at IEEE PerCom, ACM CCR, and ACM OSR. He is a member of the editorial board of the Computer Networks Journal and member of organizing and scientific committees of many international conferences.

- Peter Christen

Peter Christen is a Professor at the Australian National University (ANU) Research School of Computer Science. He graduated with a PhD in Computer Science in 1999 from the University of Basel, Switzerland, and has been at the ANU since 2000. He is a leading expert in data mining and in record linkage, the process of identifying records that correspond to the same entity across disparate databases, with a focus on privacy aspects in record linkage. He has led various research projects funded by the Australian Research Council, Google, Fujitsu Labs, and others. He is an award winning PhD supervisor who in 2014 has received the ANU Vice Chancellor's Award for Excellence in Supervision (2014). Peter has published one monograph ('Data Matching' by Springer in 2012), one edited book, eight book chapters, 22 journal articles and over one hundred fully reviewed conference and workshop papers.