The Specter of Malicious Computing

Securing the Internet of Things

The Internet of Things (IoT) is taking off, and with it the vision of pervasive computing. Internet-enabled computers are now embedded in everything from cars to pacemakers to electronic door locks to home heating controllers. Unfortunately, security, safety, and privacy considerations have lagged behind in the race to build new applications and services.

Researchers demonstrated years ago how to take control of an Internet-enabled car or hack a range of wireless medical devices. Since then, the lack of IoT security has led to numerous significant real-world attacks, such as the IoT-based Mirai botnet in late 2016 or the February 2017 denial-of-service attack on a university from its own IoT-enabled vending machines and light switches. In the near future, we will have to worry about the inappropriate or malicious use of the IoT infrastructure in our hospitals, schools, roads, and other public spaces. As more IoT deployments roll out, privacy considerations will also become more important as our personal lives are tracked in increasing detail across the physical world.

The future of pervasive computing looks bleak unless we can secure smart environments more effectively and address the major privacy challenges that come from embedded computing infrastructure. The three articles in this special issue explore promising directions for unlocking the potential of IoT technology while addressing significant safety and security concerns as well as respecting users’ privacy.

In “N-BaIoT—Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders,” Yair Meidan, Michael Bohadana, Yael Mathov, Yisroel Mirsky, Asaf Shabtai, Dominik Breitenbacher and Yuval Elovici look at methods of addressing attacks launched from large numbers of IoT devices. Using novel anomaly detection methods, they are able to quickly and accurately detect anomalous traffic from IoT devices—a vital first step toward blocking malicious traffic from compromised devices.

“IoT-Enabled Highway Maintenance: Understanding Emerging Cybersecurity Threats,” by Ludwig Trotter, Mike Harding, Mateusz Mikusz, and Nigel Davies, explores new territory in the domain of highway maintenance—a field that is surprisingly underexplored given the wealth of work on autonomous vehicle safety and security.

And in “Personalized Privacy Assistants for the Internet of Things: Providing Users with Notice and Choice,” Anupam Das, Martin Degeling, Daniel Smullen, and Norman Sadeh look at the
myriad privacy problems that the IoT may bring about. The authors then describe how augmenting IoT infrastructure to support personalized privacy assistants is a scalable way for both users and infrastructure builders to support privacy in a world where sensors and actuators abound.

We hope you enjoy this special issue and see this research as the start of our journey toward a hopeful future for the IoT and a safer, more secure, and inclusive vision of pervasive computing.

ABOUT THE GUEST EDITORS

Alastair Beresford is a reader in computer security at the University of Cambridge Computer Laboratory and an Official Fellow and Director of Studies in Computer Science at Queens’ College, Cambridge. His research examines the security and privacy of large-scale distributed computer systems. Beresford received a PhD in engineering from the University of Cambridge. Contact him at alastair@beresford.me.uk.

Cecilia Mascolo is a full professor of mobile systems in the University of Cambridge Computer Laboratory. She is also director of the Centre for Mobile, Wearable Systems, and Augmented Intelligence, a fellow of Jesus College, and a fellow of the Alan Turing Institute for Data Science in London. Mascolo received a PhD in computer science from the University of Bologna. Contact her at cecilia.mascolo@cl.cam.ac.uk.

Marco Gruteser is a professor of electrical and computer engineering and a member of the Wireless Information Network Laboratory (WINLAB) at Rutgers University. His research covers location privacy, location-aware networking, and connected vehicle applications. Gruteser received a PhD in computer science from the University of Colorado Boulder. Contact him at gruteser@winlab.rutgers.edu.