
## Call for Papers:

# The Specter of Malicious Computing:

## Securing the Internet of Things

Publication: July–September 2018 • Submission Deadline: 1 October 2017

The Internet of Things is taking off: Internet-enabled computers are now embedded in everything from cars to pacemakers, and from electronic door locks to home heating controllers. Unfortunately, security has lagged behind in the race to build new applications and services. Researchers have already demonstrated how to take control of an Internet-enabled car or hack a range of wireless medical devices. The lack of IoT security has since led to a number of 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.

The aim of this special issue is to explore new technologies, methodologies, and applications that relate to all aspects of securing future pervasive computing systems and infrastructures. Contributions might come from diverse fields such as HCI, distributed systems, dependable computing, psychology and sociology, IoT, cyber-physical systems, ubiquitous computing, ambient intelligence, legal scholarship and ethics, and economics. We welcome a wide range of research papers including descriptions of completed systems, experience reports, new insights into specific technologies and novel algorithms, and vision papers that articulate new challenges for the field.

Relevant topics for this special issue include, but are not limited to, the following:

- Analysis, detection, and prevention of IoT botnets.
- Using blockchain technology to secure the IoT.
- IoT-related ransomware, malware, and malvertisement services and architectures.
- Illicit surveillance of people and places through smart appliances and other Internet-enabled things.
- Management of the security of numerous pervasive devices across heterogeneous deployments.
- The security of safety-critical systems—such as national infrastructure (energy, transportation, payment, and so on), smart cars, and medical devices.
- Negative externalities and other economic costs of pervasive security.
- Next-generation security and privacy challenges (technical, social, economic, political, legal) in a world of smart, Internet-enabled devices.

The guest editors invite original and high-quality submissions addressing all aspects of this field, as long as the connection to pervasive computing and/or the Internet of Things is clear and central to the paper.

## Guest Editors


- Alastair Beresford, University of Cambridge
- Marco Gruteser, Rutgers University
- Marc Langheinrich, Università della Svizzera Italiana (USI)

For more information, contact the guest editors at pvc3-2018@computer.org.


## Submission Information

Submissions should be 4,000 to 6,000 words long and should follow the magazine's guidelines on style and presentation. For general author guidelines or submission details, see www.computer.org/pervasive/author.htm or pervasive@computer.org.

To submit your article to our online peer-review system, go to Manuscript Central at https://mc.manuscriptcentral.com/pc-cs.

www.computer.org/pervasive