1st IEEE Workshop on Smart City Security and Privacy

Call for papers with workshop deadlines

The world is moving to digitalization and intelligentization for the long term. We are at an important point in this evolution, as new forces emerge and combine to create new ways for cities to work. For instance, insights from information transfer across platforms can be exploited to reduce accidents, improve air quality, and alert disaster events. Cyber-physical systems (CPS) also bring new risks that arise due to the unexpected interaction within city services. These safety risks arise because of information that distracts users while driving, software errors in medical devices, corner cases in data-driven control, compromised sensors in drones or conflicts in societal policies. In parallel, artificial intelligence flourishes the development of cities, revolutionizing the way that public services are interacted with citizens. The data that drives the smarter city must be secure, to safely fuel unhindered progress.

The IEEE Workshop on Smart City Security and Privacy seeks to bring together researchers and practitioners to share their perspectives and solutions as well as deliberate on opportunities & challenges associated in the most recent synergistic Internet of Things and security and privacy. The primary objective of the “Smart City” is to improve citizens’ quality of life by providing core infrastructure – assured electricity supply, adequate and assured water supply, smart home appliance control, efficient mobility and public transportation, smart car design or conflicts, secure medical devices, digital health & online education, etc. The workshop welcomes contributions that integrate computer networking and software systems provided by disparate stakeholders, particularly those that have humans in the loop. As safety is inherently linked with the security and privacy, we also seek contributions in these areas that address safety concerns. We seek to develop a community that systematically dissects the vulnerabilities and risks exposed by these emerging cyber-physical systems, and create tools, algorithms, frameworks and systems that help in the development of safe smart cities.

The workshop covers security and privacy as well as safety topics as it relates to an individual’s health (physical, mental), the society (air pollution, toxicity, disaster events), or the environment (species preservation, global warming, oil spills), mainly from a human perspective. Our workshop will cover, but not limit itself to, the following domains: autonomous vehicles and transportation infrastructure; medical CPS and public health; smart buildings, smart grid and smart cities.

- Security and privacy of smart city networking, services and infrastructures and reliability
- Security and privacy of smart utilities, smart grid, consumption, sensing, and Internet of Things
- Security and privacy of smart city big data, open data, and urban computing
- Modeling security, safety, and privacy for smart cities
- Security and privacy of smart transportation system planning, evaluation, and technologies
- Assured smart city sewage, water and electricity management
- Smart city privacy-aware healthcare service and medical CPS
- Smart city crime watching and alerting systems
- Security and privacy of smart homes, smart building, and social community networks/infrastructures

Call for Posters and Demos
If you would like to share a provocative opinion, an interesting preliminary work, or a cool idea that will spark discussion about smart city security and privacy, the poster and demo section is a perfect venue to introduce new or ongoing work. Poster and demo presenters will have the opportunity to discuss their work, get exposure, and receive feedback from attendees.

Submission Guidelines:

Papers must be submitted via EDAS in the following link: XXXXXX

Submitted papers must be unpublished and must not be currently under review for any other publication. Submissions for full papers must be at most 6 single-spaced, double column printed pages, including all the figures, references and appendices, and not published or under review elsewhere. Submissions for Posters and Demos must be at most 1 printed page and also follow the standard IEEE Conference templates for Microsoft Word or LaTeX formats found at: https://www.ieee.org/conferences/publishing/templates.html. More information and template downloads can be found at the IEEE MASS main page.

Paper reviewing is single-blind and submissions should list author names on the front page. Papers that do not meet the size and formatting requirements will not be reviewed. All papers must be in Adobe Portable Document Format (PDF) and submitted through the web submission form.

- Full Papers: 6 pages
- Posters and Demos: 1 page

Timeline:

- Paper submission deadline: July 23, 2019
- Notification of acceptance: August 23, 2019
- Camera-ready deadline: August 30, 2019
- Workshop day: November 4, 2019

Co-Organizers:
Yuan Tian (University of Virginia)
Desheng Zhang (Rutgers University)
Jason Xue (The University of Adelaide)
Haiying Shen (University of Virginia)

Publicity Chair:
Jun Han (National University of Singapore)

Technical Program Committee:

- Chao Chen (Swinburne University of Technology, Australia)
- Emma Zhang (The University of Adelaide, Australia)
- Farhad Farokhi (The University of Melbourne, Australia)
- Muhammad Ikram (Macquarie University, Australia)

- Shiqing Ma (Rutgers University, USA)
- Shouling Ji (Zhejiang University, China)
- Xiaofei Xie (Nanyang Technological University, Singapore)
- Xin Yuan (University of Technology Sydney, Australia)
- Yan Meng (Shanghai Jiao Tong University, China)
- Yang Zhang (CISPA Helmholtz Center for Information Security, Germany)