1st ACM Workshop on the Internet of Safe Things

https://www.safethings.info/

November 5, 2017 at TU Delft, The Netherlands

Co-located with ACM SenSys 2017

Call For Papers

As the traditionally segregated systems are brought online for next generation connected applications, we have an opportunity to significantly improve the safety of legacy systems. For instance, insights from data across systems can be exploited to reduce accidents, improve air quality and support disaster events. Cyber-physical systems (CPS) also bring new risks that arise due to the unexpected interaction between systems. 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.

Accordingly, the Internet of Safe Things workshop (or SafeThings, for brevity) seeks to bring researchers and practitioners that are actively exploring system design, modeling, verification, authentication approaches to provide safety guarantees in the Internet of Things (IoT). The workshop welcomes contributions that integrate hardware and software systems provided by disparate vendors, particularly those that have humans in the loop. As safety is inherently linked with the security and privacy, we also seek contributions in security and privacy that address safety concerns. With the SafeThings workshop, we seek to develop a community that systematically dissects the vulnerabilities and risks exposed by these emerging CPSes, and create tools, algorithms, frameworks and systems that help in the development of safe systems.

SafeThings workshop covers 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). The workshop considers safety from a human perspective, and thus, does not include topics such as thread safety or memory safety in its scope.

Our workshop will cover, but not limit itself to, the following subject categories:

- Verification of safety in IoT platforms
- Privacy preserving data sharing and analysis
- Compliance with legal, health and environmental policies
- Integration of hardware and software systems
- Conflict resolution between IoT applications
- Safety in human-in-the-loop systems
- Support for IoT development - debugging tools, emulators, testbeds
- Usable security and privacy for IoT platforms
- Resiliency against attacks and faults
- Secure connectivity in IoT

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.

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 IoT safety, the poster and demo session 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. In the one page abstract, clearly explain what will be presented or demonstrated and list any requirements other than an easel and a WiFi connection.

Important Dates

Abstract Submission Deadline: July 23, 2017, 23.59 AOE
Paper Submission Deadline: July 30, 2017, 23.59 AOE
Poster and demo submission deadline: July 30, 2017, 23.59 AOE
Acceptance Notification: August 21, 2017
Camera-ready versions: September 10, 2017

Organizing Committee

General Chairs
Patrick Tague (Carnegie Mellon University)
Bharathan Balaji (University of California, Los Angeles)

Program Chairs
Mani Srivastava (University of California, Los Angeles)
Yuan Tian (Carnegie Mellon University)

Poster and Demo Chair
Houssam Abbas (University of Pennsylvania)

Publication Chair
Rasit Eskicioglu (University of Manitoba)

SenSys Workshop Chair
Xiaofan (Fred) Jiang (Columbia University, USA)

Technical Program Committee

Blase Ur (University of Chicago)
Xiao Feng Wang (Indiana Bloomington)
Xinyu Xing (Penn State)
Paulo Tabuada (University of California, Los Angeles)
Supriyo Chakraborty (IBM Research)
Muhammad Naveed (University of Southern California)
Yasser Shoukry (University of California, Berkeley)
Yuvraj Agarwal (Carnegie Mellon University)
Rajesh Gupta (University of California, San Diego)
Brad Campbell (University of Virginia)

John Stankovic (University of Virginia)
Madhur Behl (University of Virginia)
Houssam Abbas (University of Pennsylvania)
Insup Lee (University of Pennsylvania)
João Vilela (University of Coimbra)
Eric Wustrow (Colorado Boulder)
Richard Han (Colorado Boulder)
Lu Feng (University of Virginia)
Earlence Fernandes (University of Michigan)
Falko Dressler (Paderborn University)
Jie Liu (Microsoft Research)
Kay Roemer (TU Graz)
Nic Lane (University College London)
Fang-Jing Wu (NEC Lab)
Jyotirmoy Deshmukh (Toyota)
Adam Doupe (Arizona State University)
Gail-Joon Ahn (Arizona State University)
Saman Zonouz (Rutgers University)
Haixin Duan (Tsinghua University)
Yutaka Arakawa (Nara Institute of Science and Technology)
Ingrid Verbauwhede (KU Leuven)
Stefano Zanero (Politecnico di Milano)
Thorsten Holz (Ruhr University Bochum)
Amir Rahmati (University of Michigan)
Cong Zheng (Palo Alto Networks)
Chenguang Shen (Facebook)
Shaunak Mishra (Yahoo Research)

Steering Committee

John Stankovic (University of Virginia)
Lorrie Faith Cranor (Carnegie Mellon University)
Srdjan Capkun (ETH Zurich)
Rupak Majumdar (Max Planck Institute for Software Systems)