

**The Eighth IEEE International Workshop on  
Security and Privacy for Internet of Things and Cyber-Physical Systems (IoT/CPS-Security 2021)**  
*Organized in conjunction with IEEE IPCCC 2021*  
**October 29th - 31st 2021 // Austin, Texas, USA**

Recent advances in networking, communications, computation, software, and hardware technologies have revolutionized the way humans, smart things, and engineered systems interact and exchange information. The Internet of Things (IoT) and Cyber-Physical Systems (CPS), which are the major contributors to this area, will fuel the realization of this new, globally interconnected cyber-world. Yet, the success, prosperity, and advancement of IoT and CPS systems strongly depend on the security, privacy and trust of the IoT and cyber-physical devices as well as the sensitive data being exchanged. While these technologies offer a lot of new possibilities, the increasing complexity of hardware and software as well as the worldwide access increase the vulnerability to security attacks. Successful attacks targeted to IoT devices and CPS systems have in common that not only a single computer is affected, but also interconnected technical systems allowing interaction with the physical world are influenced leading to malfunction of devices and control systems with severe financial, environmental and health losses. This fact highlights the need to develop novel tools that will constitute the heart of a much-needed science of security for IoT and CPS. The goal of the IoT/CPS-Security 2021 workshop is to bring together internationally leading academic and industrial researchers in an effort to identify and discuss the major technical challenges and recent results aimed at addressing all aspects of security and privacy for IoT and CPS.

**Topics of interest**

To ensure complete coverage of the advances in this field, the IoT/CPS-Security 2021 Workshop solicits original contributions in, but not limited to, the following topical areas:

- Security, Privacy and Trust for IoT and CPS Systems
- Secure IoT and CPS architectures
- Detecting and preventing attacks in IoT devices and CPS systems
- Evaluation of the Threats, Attacks and Risks in IoT and cyber-physical devices
- Data Security and Privacy in the IoT
- Game theory for IoT and CPS security
- Security and Privacy in IoT applications and services (health care, smart cities, smart grid, etc.)
- Security and Privacy for RFID, sensors, actuator technologies
- Security in Smart Grids and Smart Spaces
- Network-distributed signal processing for security solutions in CPS
- Joint security and privacy aware protocol design
- Test-bed and performance metrics of security solutions in CPS
- Deployment and performance studies of secure CPS
- Secure network control systems for CPS applications
- Architectures for secure hardware/software CPS systems

**Submission Procedure**

The workshop accepts only novel, previously unpublished papers. All submissions should be written in English with a maximum paper length of six (6) printed pages (10-point font) including figures without incurring additional charges (maximum 1 additional page with over-length page charge if accepted). The EDAS link for submission is (TBD).

**General Co-Chairs**

Houbing Song (Embry-Riddle Aeronautical Univ.)  
Qinghe Du (Xi'an Jiaotong University)

**Technical Program Co-Chairs**

Huihui Wang (St. Bonaventure Univ.)  
Bin Jiang (Shenzhen Univ.)  
Michal Kedziora (Wroclaw Univ. of Science and Technology)

**Publicity Chair**

Jian Wang (Embry-Riddle Aeronautical Univ.)

**Important Dates**

Submission Deadline: August 1, 2021  
Acceptance Notification: August 20, 2021  
Camera Ready: September 5, 2021  
Workshop date: October 31, 2021