Call for Contributions

Submission:
1. Inform the Chairs: with the Title of your Contribution
2. Submission URL:
https://www.iariasubmit.org/conferences/submit/newcontribution.php?event=ICSEA+2019+Special
Please select Track Preference as **CPSSEC**

Special track

CPSSEC: Security in Cyber Physical Systems

Chairs and Coordinators

Rohith Yanambaka Venkata, University of North Texas, USA
rohithyanambakavenkata@my.unt.edu

Dr. Krishna Kavi, University of North Texas, USA
Krishna.kavi@unt.edu

along with
ICSEA 2019, The Fourteenth International Conference on Software Engineering Advances
November 24, 2019 to November 28, 2019 - Valencia, Spain
https://www.iaria.org/conferences2019/ICSEA19.html

Cyber Physical Systems (CPS) are a unique blend of computational and physical systems designed to interact with the physical world. They are typically composed of sensors, actuators, network equipment and control processing units. The proliferation of CPS has gained increased traction with the advances in networking and embedded system technologies like Systems-on-Chip (SoC) and wireless transceivers. This widespread growth of cyber and physical system technologies is creating several new applications in areas such as autonomous vehicles and smart infrastructure, where domain-specific, proprietary technologies are required to help meet the design goals.

While the unique confluence of cyber and physical systems is ideal for fast-moving markets, their heterogeneous nature introduces several challenges, with security being the chief among them. Many CPS applications, such as smart grids and water treatment plants are safety-critical: their failure may cause irrevocable harm to the physical systems under control and to people who rely on and operate them. Securing these CPS infrastructures is therefore, paramount. Security issues must be analyzed, understood and addressed not only in the early stages of design and development, but throughout the entire lifecycle of the CPS system. Incorporating security in Product Lifecycle Management (PLM) ensures protection against an ever evolving threat landscape.

CPS systems are often designed to collect large amounts of sensor data non-intrusively to achieve seamlessness. The users of these applications are often oblivious to the blatant disregard for data privacy. Hence, CPS system must also be designed with privacy considerations in addition to security.

To help address these concerns, we invite original contributions on the security and privacy of Cyber Physical Systems.

Topics include, but not limited to:

- Translating functional requirements/design goals to security requirements
- Design framework for CPS with a focus on security as a fundamental design goal
- Mathematical foundations to secure CPS
- Control theoretic approach to secure CPS
- Privacy in CPS
- Resiliency in CPS
- Secure CPS architectures
- Authentication mechanisms for CPS
- Access control for CPS
- Key management in CPS
- Data security and privacy for CPS
- Availability, recovery and auditing for CPS
- Threat models for CPS
- Vulnerability analysis for CPS
- Anonymization in CPS
- Security in industrial control systems
- Physical layer security for CPS
- Hardware security in CPS

Important Datelines

Inform the Chair (see Contacts below): as soon as you decide to contribute
Submission: Sep 18, 2019
Notification: Oct 17, 2019
Registration: Oct 27, 2019
Camera-ready: Oct 27, 2019

Contribution Types
- Regular papers [in the proceedings, digital library]
- Short papers (work in progress) [in the proceedings, digital library]
- Posters: two pages [in the proceedings, digital library]
- Posters: slide only [slide-deck posted on www.iaria.org]
- Presentations: slide only [slide-deck posted on www.iaria.org]
- Demos: two pages [posted on www.iaria.org]

Paper Format
- See: http://www.iaria.org/format.html
- Before submission, please check and comply with the editorial rules: http://www.iaria.org/editorialrules.html

Publications
- Extended versions of selected papers will be published in IARIA Journals: http://www.iariajournals.org
- Print proceedings will be available via Curran Associates, Inc.: http://www.proceedings.com/9769.html
- Articles will be archived in the free access ThinkMind Digital Library: http://www.thinkmind.org

Paper Submission
https://www.iariasubmit.org/conferences/submit/newcontribution.php?event=ICSEA+2019+Special
Please select Track Preference as **CPSSEC**

Registration

- Each accepted paper needs at least one full registration, before the camera-ready manuscript can be included in the proceedings.
- Registration fees are available at http://www.iaria.org/registration.html

Contacts

Rohith Yanambaka Venkata: rohithyanambakavenkata@my.unt.edu
Krishna Kavi: Krishna.kavi@unt.edu
Logistics: steve@iaria.org