Call for Contributions

Submission:
1. Inform the Chair: with the Title of your Contribution
2. Submission URL:
Please select Track Preference as **SECIoT**

Special track

SECIoT: Security and Privacy in the Internet of Things (IoT)

Chair and Coordinator

Tal Melamed, FBK, the Security & Trust Research Unit, Italy |
AppSec Labs, Security Academy, Israel
tal@appsec.it

along with

SECURWARE 2018, the Twelfth International Conference on Emerging Security Information, Systems and Technologies
September 16, 2018 to September 20, 2018 - Venice, Italy
http://www.iaria.org/conferences2018/SECURWARE18.html

The Internet of Things (IoT) is an integral part in our everyday lives. Broadly used in the healthcare, fitness, security, home-entertainment, critical infrastructures and other sectors, nowadays we encounter IoT in almost every aspect of our lives (e.g. in wearables, sensors, medical devices, security products, etc.), allowing the exchange of information between people, devices, and infrastructures. However, despite the serious impact that IoT vulnerabilities may have on us, the security and privacy are sometime left behind.

In this special track, we decided to focus on novel methodologies, concepts and tools for the protection of IoT technologies. The objective is to discuss security and privacy implications of IoT technologies from different fields of application, such as physical, cyber and societal aspects. In this context, we are interested in conceptual work (e.g., frameworks and best practices), technical solutions (e.g., tools and prototypes), as well as empirical studies.

Topics include, but not limited to:
- IoT security services and applications
- Cyber intelligence techniques for IoT
- Industrial IoT security
- Open Source IoT
- Blockchain and IoT
- Connected/Smart Cities
- Security and Privacy in Smart medical devices
- Effect of GDPR on IoT Security
- IoT forensics; Connected-Cars security
- Secure mobile technologies for IoT
- Malware in IoT applications
- IoT infrastructures and mitigation techniques
- Vulnerability analysis and Reverse engineering for IoT
- Intrusion detection and prevention for IoT

- Denial of Service (DoS) attacks for IoT
- IoT cyber crime
- Smart grid security
- Threat Models in IoT
- Security in wireless sensor networks
- Identity management in IoT
- Cryptography protocols and algorithms for IoT
- Privacy and security issues of smart-home systems
- Security in wireless Point-of-Sales (WPOS)
- Challenges and recommendations for IoT
- Architecture for secure IoT

Important Datelines
- Inform the Chair (see Contacts below): as soon as you decided to contribute
- Submission: ~~June 1~~ July 10
- Notification: ~~July 2~~ July 30
- Registration: ~~July 16~~ August 10
- Camera ready: ~~July 22~~ August 10

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=SECURWARE+2018+Special
Please select Track Preference as **SECIoT**

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
Chairs: Tal Melamed, tal@appsec.it
SECURWARE logistics: steve@iaria.org