SPECIAL SESSION or WORKSHOP ON

Cyber Security Systems

IEEE SOSE'20

June 2-4, 2020, Budapest, Hungary

Proposers

Valéria Póser
Óbuda University, Hungary, Email:
poser.valeria@nik.uni-obuda.hu

Prof. Zoltán Rajnai
Óbuda University, Hungary, Email:
rajnai.zoltan@bgk.uni-obuda.hu

Anna Bánáti
Óbuda University, Hungary, Email:
banati.anna@nik.uni-obuda.hu

Miklos Kozlovszky
Óbuda University, Hungary, Email:
kozlovszky.miklos@nik.uni-obuda.hu

Description: Over the past decade, our connected world and the large amount of stored data, have dramatically increased the attack surface of consumers, the enterprise networks and critical infrastructure systems. New sophisticated attacks and threats are being discovered day after day while their detection and the defense require more and more specialized tools, methods and techniques. Numerous new methods, threat hunting techniques, machine learning algorithms and data mining techniques have found their ways in the field of cyber-security in order to identify new and unknown malware, improve intrusion detection systems, enhance spam detection, or prevent software exploit to execute.

Scope: This special session on cyber security is aimed at academic researcher applying improved traditional and non-traditional methods, techniques and applications to solve system level cyber-security problems from the different aspects.

Key words: Original papers are invited from multidisciplinary perspectives on subject areas including, but not limited to:

- Tools and Techniques:
  - Threat Hunting
  - Malware Analysis & Detection
  - Forensics Investigation
  - Cyber Threat Intelligence
  - Intrusion detection and Incident Response
  - Visualization techniques for intelligence analysis and investigation
  - Log Analysis
  - Phishing and Spear-Phishing detection and Prevention
- Data and Data Science:
  - Models for forecasting cyber-attacks and measuring impact
  - Models for attack-pattern recognition
  - Data representation
  - Data simulation
  - Data collection, filtering and storage analysis
  - New formats and Taxonomies
- Methods and Algorithms:
  - Challenges of Machine Learning for Cyber Security
  - Machine learning algorithms for detection and recognition
  - Graph Representation Learning
  - Scalable Machine Learning for Cyber Security
  - Neural Graph Learning
  - Machine Learning Threat Intelligence

SUBMISSION: Papers must be submitted electronically for peer reviews by **March 15, 2020**. All papers must be written in English and should describe original work.

DEADLINES

Full paper submission March 1, 2020

Notification April 1, 2020

Final paper submission April 30, 2020