

Call for Papers

ACM Transactions on Intelligent Systems and Technology ([ACM TIST](#))

Special Issue on Cyber Security

Overview

Computer and communication systems are subject to repeated security attacks. It is not surprising that the field of computer and network security has grown and evolved significantly in recent years given the variety of new vulnerabilities discovered daily, the introduction of new attack schemes, and the ever-expanding use of the Internet. A highly dynamic threat landscape has emerged due to the evolution in the types of attacks administered, such as Advanced Persisted Threats (APTs), as well as attacks against embedded devices connected to the internet, and the identification of new vulnerabilities. These developments pose new threats for which traditional security approaches are ill-equipped.

In recent years, various computational intelligence techniques have been used to develop powerful solutions for coping with the latest threats, such as: distributed denial of service (DDoS) attacks, APTs, host-based intrusions, data leakage, and malicious code. Given the growing interest in the field, it is not surprising that a variety of methods are now being employed by researchers and practitioners. Since the field is extremely dynamic, the academic community increases the invested research in cyber, and leading journals designate editions and issues to this subject. This special issue will focus on presenting innovative technologies for coping with the latest cyber security challenges.

Topics of Interests

We invite the submission of high-quality manuscripts that report relevant research in the areas of benchmarking and the evaluation of recommendation systems. This special issue welcomes submissions which present technical, experimental, methodological and/or applicative contributions within this scope, addressing—though not limited to—the following topics:

- Data, computer, and network security
- Hardware and embedded systems security
- Cybersecurity oriented cryptography and cryptanalysis
- Trusted protocols certificates and authentication
- Design and analysis of security mechanisms
- Security of cyber-physical systems and national infrastructures
- Security of smart-cities and Internet of Things
- Human interaction and usability aspects of cyber security
- Privacy and personal data in cyberspace
- Counter data-leakage methodologies
- Anonymization and sanitization
- Cybersecurity and artificial intelligence
- New cyber-security threats

Submissions

Manuscripts shall be sent through the ACM TIST electronic submission system at <http://mc.manuscriptcentral.com/tist> (please select "Special Issue: Cyber Security" as the manuscript type). Submissions shall adhere to the ACM TIST instructions and guidelines for authors are available at the journal website: <http://tist.acm.org>.

The papers will be evaluated for their originality, contribution significance, soundness, clarity, and overall quality. The interest of contributions will be assessed in terms of technical and scientific findings, contribution to the knowledge and understanding of the problem, methodological advancements, and/or applicative value.

Important Dates

Paper submission due:	February 1 st , 2015
First round of reviews:	April 15 th , 2015
First round of revisions:	May 15 th , 2015
Second round of reviews:	June 15 th , 2015
Final round of revisions:	July 15 th , 2015
Final paper notification:	August 15 th , 2015
Camera-ready due:	September 2015

Guest Editors

Yaniv Harel: Tel-Aviv University (& EMC)

- Yaniv Harel, Research Director, Blavatnik Cyber Center, Tel-Aviv University
- Yaniv.c.harel@gmail.com

Irad Ben-Gal: Tel-Aviv University

- bengal@tauex.tau.ac.il
- <http://www.eng.tau.ac.il/~bengal/>

Yuval Elovici: Ben-Gurion University

- elovici@bgu.ac.il
- <http://Tlabs.bgu.ac.il/yuval>