Call for Papers

Journal of Universal Computer Science (J.UCS) Special Issue

Technical and Social Aspects of Critical Infrastructure Security

Guest Editors:

Jörg Keller
Faculty of Mathematics and Computer Science
University of Hagen
joerg.keller@fernuni-hagen.de

Igor Bernik
Faculty of Criminal Justice and Security
University of Maribor
igor.bernik@fvv.uni-mb.si

Wojciech Mazurczyk
Faculty of Electronics and Information Technology
Warsaw University of Technology
wmazurcz@elka.pw.edu.pl

Background & Call for Manuscripts

Critical infrastructure has several sectors whose assets, systems, physical and virtual networks are considered so vital to a country that their destruction or incapacitation would have a debilitating effect on security, economic security, public health or any combination thereof. Critical infrastructure includes the communications sector, the chemical sector, the commercial facilities sector, the critical manufacturing sector, the defense industrial base sector, the emergency services sector, energy sector, the financial services sector, the food and agriculture sector, the government facilities sector, the healthcare sector, the information technology sector, the transportation systems sector, the water and wastewater systems sector, and the nuclear reactors, materials and waste sector. Today, all critical infrastructure sectors rely heavily on IT for operations. The critical infrastructure security however remains a major challenge. As shown by the latest global ransomware attacks, both social and technical shortcomings play important roles in achieving adequate levels of critical infrastructure (in)security. For example, targeted attacks exploiting social shortcomings may be used to first penetrate into a critical infrastructure system, and then spread like wildfire by exploiting its technical shortcomings.

This special issue targets security of all types of critical infrastructure. Research papers can address both social and technical aspects of ensuring critical infrastructure security.

Topics of interest include, but are not limited to:

- Cyber resilience of employees in critical infrastructure sectors
- Critical infrastructure cyber attack vectors
- Business continuity and ransomware recovery

- Blockchain and critical infrastructure security
- Embedded security in critical infrastructures
- Vulnerability and risk assessment methodologies for distributed critical infrastructures
- Simulation and test beds for the security evaluation of critical infrastructures
- Cyber-physical systems security approaches and algorithms
- Critical infrastructure security policies, standards and regulations
- Cyber security for critical infrastructures including health and banking systems
- Cyber security of complex and distributed critical infrastructures
- Cyber security of industrial control systems
- Security of the smart grid
- Security of supervisory control and data acquisition (SCADA) systems
- Critical infrastructure IoT security
- Critical software security
- Critical infrastructure cyber warfare
- Ethical and legal limitations of attack retaliation measures
- Critical infrastructure surveillance, interception, blocking and sovereignty

Important Deadlines

Submission by:	~~8 January 2018~~	**22 January 2018**
Notification of authors by:	~~12 February 2018~~	**19 February 2018**
Revised submission by:	16 April 2018	
Notification about final decision by:	21 May 2018	

Submission and Evaluation Procedure

The Journal of Universal Computer Science is a high-quality electronic publication that deals with all aspects of computer science. J.UCS has been appearing monthly since 1995 and is thus one of the oldest electronic journals with uninterrupted publication since its foundation. A number of special issues as well as the printed archive editions of the volumes are also available in print and can be ordered directly from J.UCS office. The impact factor of J.UCS is 0.546, the 5-year impact factor 0.684 (2015). For further information, please refer to

http://www.jucs.org/jucs_info/aims/unique_features.html

Manuscripts must be submitted in PDF format, written in English and should not exceed 20 pages. Papers only prepared according to the JUCS's guidelines for authors and submitted online (see procedure described below) will be included in the review process. Illustrations and tables must be provided as integrated parts of the manuscript. The guidelines for authors are available at

http://www.jucs.org/ujs/jucs/info/submissions/style_guide.html.

For all potential authors who have received an invitation for an extended version of their CECC 2017 paper, please bear in mind that we can only consider submissions which are significantly extended (at least 50 percent new material and the title of the extended version must clearly and unmistakably differ from the title of the article presented at the conference). Only novel research papers which are currently not under review at another event or a journal are accepted for the review process. For more details, please also refer to

http://www.jucs.org/ujs/jucs/info/special_issues/special_guidelines.html.

Please submit your original and proof-read papers not later than 8 January 2018 using the submission system at (https://easychair.org/conferences/?conf=tasacis2018). Each paper will be blind reviewed by at least 3 reviewers. According to the covered main subjects in the content, a selected set of reviewers with the appropriate expertise will be assigned.

Program Committee

Prof. Dr. Miroslav Bača, University of Zagreb, Croatia
Prof. Dr. Igor Bernik, University of Maribor, Slovenia
Dr. Krzysztof Cabaj, Warsaw University of Technology, Poland
Dr. Luca Caviglione, ISSIA, CNR, Italy
Prof. Dr. Michal Choras, University of Technology and Life Sciences, Poland
Prof. Dr. Tobias Eggendorfer, Univ. Appl. Science Ravensburg-Weingarten, Germany
Dr. Bela Genge, University of Tg. Mures, Romania
Prof. Dr. Christian Hummert, Univ. Appl. Science Mittweida, Germany
Prof. Dr. Jörg Keller, University of Hagen, Germany
Dr. Maciej Korczynski, Delft University of Technology, The Netherlands
Dr. Jean-Francois Lalande, Inria, Univ. Rennes 1, INSA Centre Val de Loire, Univ. Orlaeans, France
Prof. Dr. Olaf Maennel, Tallinn Tech University, Estonia
Dr. Jorge T. Martins, University of Sheffield, United Kingdom
Dr. Blaž Markelj, University of Maribor, Slovenia
Prof. Dr. Wojciech Mazurczyk, Warsaw University of Technology, Poland
Dr. Roman Messmer, ORF, Austria
Dr. Kai Simon, Kai Simon Consulting, Germany
Prof. Dr. Mark Strembeck, WU Wien, Austria
Dr. Simon Vrhovec, University of Maribor, Slovenia
Prof. Dr. Damian Weber, Univ. Appl. Science Saarbrücken, Germany
Prof. Dr. Steffen Wendzel, Worms University of Applied Science, Germany
Prof. Dr. Dirk Westhoff, Univ. Appl. Science Offenburg, Germany