Journal of Universal Computer Science

Special issue on

Recent Advances in Detection, Investigation and Mitigation of Cyber Crimes

Call for papers

Guest editors

Artur Janicki (lead)
Warsaw University of Technology, Warsaw, Poland
email: A.Janicki@tele.pw.edu.pl

Wojciech Mazurczyk
Warsaw University of Technology, Warsaw, Poland
email: W.Mazurczyk@tele.pw.edu.pl

Xiangyang Luo
Zhengzhou Information Science and Technology Institute, Zhengzhou, China
email: luoxy_ieu@sina.com

Dengpan Ye
Wuhan University, Wuhan, China
email: yedp2001@163.com

Deadlines

Submission by:	14 January 2019
Notification of authors by:	1 April 2019
Revised submission by:	31 May 2019
Notification about final decision by:	5 July 2019
Planned publication in J.UCS:	Autumn 2019

Background information

Today's world's societies are becoming more and more dependent on open networks such as the Internet – where commercial activities, business transactions and government services are realized. This has led to the fast development of new cyber threats and numerous information security issues which are exploited by cyber criminals. The inability to provide trusted secure services in contemporary computer network technologies has a tremendous socio-economic impact on global enterprises as well as individuals.

Moreover, the frequently occurring international frauds impose the necessity to conduct the investigation of facts spanning across multiple international borders. Such examination is often subject to different jurisdictions and legal systems. A good illustration of the above being the Internet, which has made it easier to perpetrate traditional crimes. It has acted as an alternate avenue for the criminals to conduct their activities, and launch attacks with relative anonymity. The increased complexity of the communications and the networking infrastructure is making investigation of the crimes difficult. Traces of illegal digital activities are often buried in large volumes of data, which are hard to inspect with the aim of detecting offences and collecting evidence. Nowadays, the digital crime scene functions like any other network, with dedicated administrators functioning as the first responders.

This poses new challenges for law enforcement policies and forces the computer societies to utilize digital forensics to combat the increasing number of cybercrimes. Forensic professionals must be fully prepared in order to be able to provide court admissible evidence. To make these goals achievable, forensic techniques should keep pace with new technologies.

The aim of this J.UCS special issue is to show the latest research results in the field of digital forensics and to present the development of tools and techniques, which assist the investigation process of potentially illegal cyber activity. We encourage prospective authors to submit related distinguished research papers on the subject of both: theoretical approaches and practical case reviews.

Topics of interest

Topics of interest include, but are not limited to:

- Ransomware: evolution, functioning, types, etc.
- Crime-as-a-service
- Criminal use of IoT e.g. IoT-based botnets
- Mobile malware
- Novel techniques in exploit kits
- Criminal to criminal (C2C) communications
- Criminal to victim (C2V) communications
- Darknets and hidden services
- Criminal abuse of clouds and social networks
- Cybercrimes: evolution, new trends and detection
- Cybercrime related investigations
- Privacy issues in digital forensics
- Network traffic analysis, traceback and attribution
- Incident response, investigation and evidence handling

- Integrity of digital evidence and live investigations
- Identification, authentication and collection of digital evidence
- Anti-forensic techniques and methods
- Watermarking and intellectual property theft
- Steganography/steganalysis and covert/subliminal channels
- Network anomalies detection
- Novel applications of information hiding in networks
- Political and business issues related to digital forensics and anti-forensic techniques

Submission Guidelines

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 the 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. Only papers prepared according to the J.UCS'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 IWCC 2018 paper, please bear in mind that we can only consider submissions which are significantly extended (at least 50% 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. All submissions based on the topics of interest must be in the main focus of computer science. 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 14 January 2019 using the submission system at https://easychair.org/conferences/?conf=radimcc2019. 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.