Call for Papers

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

Cyberattack Detection and Response

Guest Editors:

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

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

Béla Genge
Department of Computer Science, Faculty of Science and Letters
Petru Maior University of Tg. Mures, Romania
bela.genge@ing.upm.ro

Lothar Fritsch
Department of Mathematics and Computer Science
Karlstad University, Germany
lothar.fritsch@kau.se

Simon Vrhovec
Faculty of Criminal Justice and Security
University of Maribor, Slovenia
simon.vrhovec@fvv.uni-mb.si

Background & Call for Manuscripts

Cyberattacks have evolved into a threat for modern society, as they affect both individuals and organizations alike. Attacks can have a multitude of different forms, ranging from denial of service to ransomware, and target government, critical infrastructure, businesses or private environments. As this threat cannot be ignored, it should be detected as early as possible, to prevent damage as much as possible. As attacks often employ multiple stages, that compromise more and more machines and/or remove more and more lines of defense, early detection seems all the more necessary. At the same time, attacks, especially if evolving over many weeks, try to stay undetected and hence employ many measures in order not to raise suspicion, which renders detection a difficult endeavor. When an attack is detected, an appropriate response is necessary, which can be as straightforward and painful as

disconnecting the victim from the net, but also can take many other forms, up to offensive countermeasures that try to attack the attacker. Both attacks and countermeasures include technical and social means, as it is sometimes easier to find out e.g. the structure of a company network by interviewing careless employees than by doing a reconnaissance.

Hence, this special issue targets actual research on the detection of and response to cyberattacks on all levels, e.g. individuals, organizations, ISPs, critical infrastructure. Research papers can address technical and/or social aspects of cyberattack detection and response, so e.g. social engineering and spear phishing detection are within the scope of the special issue.

Topics of interest include, but are not limited to:

- Malware presence detection (e.g., covert communication) at organizational and ISP levels
- Malware activation detection and response (e.g., ransomware)
- Malware propagation detection and blocking (e.g., network-based malware detection and responses)
- Botnet detection
- Response to DDoS attacks, especially in critical infrastructure sectors
- Detection of compromised network infrastructure (e.g., DNS spoofing) at organizational and ISP levels
- Technical detection of social components of cyberattacks (e.g., spear phishing, social engineering) and countermeasures
- Human-based detection of social components of cyberattacks (e.g., awareness, training, motivation)
- Detection of malicious actions by organizational insiders (technical and human-based)
- Cyber resilience of organizational insiders, especially in critical infrastructure sectors
- Detection of cyber-physical attacks on smart systems (e.g., smart home burglary prevention)
- Impact of detection and response measures on the investigation of cyberattacks
- Detection and response to cyber-physical attacks on critical infrastructure
- Cyberattack countermeasures, especially offensive responses

Important Deadlines

Submission by:	15 February 2019
Notification of authors by:	25 April 2019
Revised submission by:	10 June 2019
Notification about final decision by:	25 July 2019

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 0.696, the 5-year impact factor 0.770 (2016). 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 2018 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 15 February 2019 using the submission system at https://easychair.org/conferences/?conf=cyder2019. 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
Prof. Dr. Luca Caviglione, ISSIA, CNR, Italy
Prof. Dr. Michal Choras, University of Technology and Life Sciences, Poland
Dr. Boštjan Delak, Faculty of Information studies in Novo mesto, Slovenia
Prof. Dr. Jan Eloff, University of Pretoria, South Africa
Dr. Bela Genge, University of Tg. Mures, Romania
Dr. Petra Grd, University of Zagreb, Croatia
Dr. Georgios Karopoulos, Joint Research Centre, Italy
Prof. Dr. Stefan Katzenbeisser, Technische Universität Darmstadt, Germany
Prof. Dr. Bradley A. Malin, Vanderbilt University, USA
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
Dr. Blaž Markelj, University of Maribor, Slovenia
Dr. Jorge T. Martins, University of Sheffield, United Kingdom
Prof. Dr. Wojciech Mazurczyk, Warsaw University of Technology, Poland
Dr. Pal-Stefan Murvay, Politechnical University of Timisoara, Romania
Prof. Dr. Haller Piroska, Petru Maior University of Tirgu Mures, Romania
Dr. Kaja Prislan, University of Maribor, Slovenia
Dr. Gerardo I. Simari, Universidad Nacional del Sur in Bahía Blanca and CONICET, Argentina
Prof. Dr. Mark Strembeck, WU Wien, Austria
Dr. Hui Tian, National Huaqiao University, China
Dr. Simon Vrhovec, University of Maribor, Slovenia
Dr. Edgar R. Weippl, SBA Research, Austria
Prof. Dr. Steffen Wendzel, Worms University of Applied Science, Germany
Prof. Dr. Christos Xenakis, University of Piraeus, Greece
Prof. Dr. Aleš Završnik, Institute of Criminology at the Faculty of Law Ljubljana, Slovenia