


Editorial: Fighting Cybersecurity Risks from a Multidisciplinary Perspective

J.UCS Special Issue


Steffen Wendzel

(Hochschule Worms, Worms, Germany)

 <https://orcid.org/0000-0002-1913-5912>, Wendzel@hs-worms.de


Aleksandra Mileva

(Goce Delcev University in Stip, Republic of N. Macedonia)

 <https://orcid.org/0000-0003-0706-6355>, Aleksandra.Mileva@ugd.edu.mk


Virginia N. L. Franqueira

(University of Kent, Canterbury, UK)

 <https://orcid.org/0000-0003-1332-9115>, V.Franqueira@kent.ac.uk

Martin Gilje Jaatun

(University of Stavanger, Norway)

 <https://orcid.org/0000-0001-7127-6694>, Martin.G.Jaatun@uis.no

Digitization, powered by the Internet, artificial intelligence, inter-operable data formats and communication standards, high-bandwidth mobile technology, and nano-technology, allows for an increasing number of new services that are tailored to the particular demands of end-users, industry and government organizations.

However, these new digital services have also become the major focus of cyber-crime. Whereas traditional research mostly covered pure technical aspects of cybercrime, it is becoming increasingly important to address cybercrime and cybersecurity in a multidisciplinary fashion, including legal, behavioral, technical and sociological aspects.

This special issue aims to offer a mixture of selected extended versions of papers presented at the European Interdisciplinary Cybersecurity Conference (EICC'23), which took place in Stavanger, Norway, as well as submissions from an open call. We considered papers dealing with the above-mentioned risks and problems, new challenges, interdisciplinary issues, and innovative multidisciplinary solutions (defense mechanisms, methods, and countermeasures) for promoting cybersecurity in the cyberspace.

Overall, we received 15 submissions. Each accepted paper received at least three reviews. After a first round of reviews, eight were rejected. The remaining seven papers underwent another round of reviews (five papers underwent a major revision and only two papers were scheduled to undergo a minor revision). Finally, the authors of these seven papers adequately addressed the reviewers' comments and they thus have been accepted for inclusion in this special issue.

We like to thank all authors who submitted their work to this special issue and all reviewers for their contributions. Further, we like to thank the J.UCS team for accepting our special issue for inclusion in their journal. We hope that all readers will enjoy this special issue.

Steffen Wendzel, Aleksandra Mileva,
Virginia N. L. Franqueira & Martin Gilje Jaatun

Papers in this special issue

The following papers have been included in this issue.

Yashovardhan Sharma, Simon Birnbach, and Ivan Martinovic show how extensible and explainable malware detection is feasible. To this end, they make use of the TTPs (Tactics, Techniques, and Procedures) of the MITRE ATT&CK framework.

Next, Orçun Çetin, Emre Ekmekcioglu, Budi Arief, and Julio Hernandez-Castro focus on the programming language PHP and perform an empirical evaluation of large language models in static code analysis for vulnerability detection.

Javier Muñoz-Calle, Rafael Estepa, Antonio Estepa Alonso, Jesús Díaz-Verdejo, Elvira Castillo-Fernández, and Germán Madinabeitia present work on an architecture for MITRE ATT&CK model-driven alerts and events correlation.

A paper by Dagmar Gesmann-Nuissl, Ines Maria Tacke, and Stefanie Meyer focuses on legal aspects of Internet-based data sharing for IoT devices as these generate data that is later processed and shared.

A paper by Lasse Nitz and Avikarsha Mandal investigates the training of domain generation algorithm (DGA) detection classifiers in a Machine-Learning-as-a-Service (MLaaS) setting.

Robin Duraz, David Espes, Julien Francq, and Sandrine Vaton study how using the Common Vulnerability Scoring System (CVSS) can improve Intrusion Detection systems in terms of training, improved evaluation of performance, and taking into account different protection requirements.

Finally, Alex Crgol and Simon Vrhovec delve into the problem faced by end-users of recognizing phishing emails, challenging the value of training users to see the difference between phishing and genuine emails.

Reviewers of this special issue

Jurlind Budurushi, DHBW Karlsruhe
Marijke Coetzee, North-West University
Tobias Eggendorfer, TH Ingolstadt
Damjan Fujs, University of Ljubljana
Lenzini Gabriele, SnT/University of Luxembourg
Dieter Gollmann, Hamburg University of Technology
Petra Grd, University of Zagreb
Nils Gruschka, University of Oslo
Piroska Haller, Petru Maior University
Marko Hölbl, Univerza v Mariboru
Sokratis Katsikas, Norwegian University of Science and Technology
Stefan Katzenbeisser, University of Passau
Joseph Kearney, University of Kent
Jean-Francois Lalande, CentraleSupélec

Shujun Li, University of Kent
Haibing Lu, Santa Clara University
Olaf Maennel, Tallinn University of Technology
Brad Malin, Vanderbilt University
David Megias, Universitat Oberta de Catalunya (UOC)
Rodrigo Miani, Federal University of Uberlândia (UFU)
Pal-Stefan Murvay, Politehnica University of Timisoara
Marek Pawlicki, Bydgoszcz University of Science and Technology
Ciara Rafferty, Queen's University Belfast
Helena Rifà-Pous, Universitat Oberta de Catalunya (UOC)
Gerardo Simari, Universidad Nacional del Sur (UNS) and CONICET
Kai Simon, Fraunhofer-Gesellschaft
Daniel Spiekermann, FH Dortmund
Hung-Min Sun, National Tsing Hua University
Igor Tomicic, University of Zagreb
Edgar Weippl, University of Vienna
Christos Xenakis, University of Piraeus
Marco Zuppelli, Institute for Applied Mathematics and Information Technologies