Journal of Universal Computer Science, vol. 26, no. 7 (2020), 762-763
submitted: 12/5/20, accepted: 28/5/20, appeared: 28/7/20

Information Security Methodology, Replication Studies and Information Security Education

J.UCS Special Issue

Steffen Wendzel
(Fraunhofer FKIE & Worms University of Applied Sciences, Germany
wendzel@hs-worms.de)

Luca Caviglione
(Institute for Applied Mathematics and Information Technologies, Italy
luca.caviglione@ge.imati.cnr.it)

Alessandro Checco
(University of Sheffield, United Kingdom
a.checco@sheffield.ac.uk)

Aleksandra Mileva
(University Goce Delcev, Macedonia
aleksandra.mileva@ugd.edu.mk)

Jean-Francois Lalande
(CentraleSupélec, France
jean-francois.lalande@irisa.fr)

Wojciech Mazurczyk
(Warsaw University of Technology, Poland
w.mazurczyk@tele.pw.edu.pl)

In recent years, research started to focus on the scientific fundamentals of information security. These fundamentals include several important aspects such as the unified description of attacks and countermeasures, the reproducibility of experiments and means to achieve this reproducibility, the sharing of research data and code, the discussion of quality criteria for experiments and the design and implementation of testbeds. The related academic publications contribute to the advancement of information security research by making possible the comparison and the benchmarking of different security solutions. As a complementary approach, works on terminology and taxonomy address redundancies and unify the understanding between different sub-domains of information security.

This special issue contains works from an open call as well as selected extended papers of the *First International Workshop on Information Security Methodology and*

Replication Studies (IWSMR), co-organized with ARES 2019. Authors of IWSMR papers provided at least 50% new content and new contributions were received. After the first round of reviews, one paper was accepted for this special issue. After another round of reviews, three additional papers were accepted.

In their paper *Bibliometric Mapping of Research on User Training for Secure Use of Information Systems*, Damjan Fujs, Simon Vrhovec and Damjan Vavpotič conduct a bibliometric mapping of research on user training for secure use of information systems.

Caroline Moeckel is the author of the paper *(De-)Constructing Attacker Categorisations: A Typology Iteration for the Case of Digital Banking.* She proposes an experimental construction of a new attacker typology grounded in real-life data.

The paper entitled *Utilizing the Debugging Information of Applications in Memory Forensics* by Mohammed Al-Saleh, Ethar Qawasmeh and Ziad Al-Sharif proposes a general solution to investigate applications resting in memory for forensics.

Finally, Anže Mihelič, Damjan Fujs, Luka Jelovčan and Simon Vrhovec propose a reasonably light-weight structure-based approach for evaluating case study and action research reports (SAE-CSAR) based on eight key parts of a real-world research report in their paper *Evaluating case study and action research reports: Real-world research in cybersecurity*.

We would like to express our thanks to the reviewers of this special issue: Krzysztof Cabaj, Mehdi Chourib, Bernhard Fechner, Bela Genge, Nils Gruschka, Thomas Kemmerich, Hanno Langweg, Olaf Maennel, Michael Meier, Slobodan Petrovic, Michael Rademacher and Simon Vrhovec.