Guest editorial: Information security methodology and replication studies

Steffen Wendzel, Luca Caviglione, Aleksandra Mileva, Jean-François Lalande, Wojciech Mazurczyk

Editorial

Steffen Wendzel*, Luca Caviglione, Aleksandra Mileva, Jean-Francois Lalande, and Wojciech Mazurczyk

Guest editorial: Information security methodology and replication studies

https://doi.org/10.1515/itit-2022-0016
Received February 22, 2022; accepted February 22, 2022

Abstract: This special issue presents five articles that address the topic of replicability and scientific methodology in information security research, featuring two extended articles from the 2021 International Workshop on Information Security Methodology and Replication Studies (IWSMR). This special issue also comprises two distinguished dissertations.

Keywords: Replicability, Experimental Design, Research Methodology, Cyber Security, Security Datasets

ACM CCS: Social and professional topics, Computing methodologies, General and reference → Cross-computing tools and techniques → Experimentation, General and reference → Cross-computing tools and techniques → Evaluation, General and reference → Cross-computing tools and techniques → Metrics

1 Replicability & scientific methodology

Research in information security has to assess proposals with large-scale experiments and scientists commonly handle large datasets, for example, security logs, source or binary codes, and network traces. In addition, the need for distributing and sharing these research artifacts with the scientific community is increasing as later contributions often require to replicate, modify or extend previous experiments. Replicating a study is also of independent interest, as black box techniques, for example, based on artificial intelligence technologies, are often employed for evaluating detection and classification methods. For all these reasons, this special issue focuses on contributions to formalize methods for comparing and evaluating research methods in information security.

In addition to open-access initiatives from major publishers for security-related articles, data and software used for published studies are becoming submission or post-proceedings artifacts. As an example, the ACSAC conference introduced in 2017 an artifact submission track for evaluating the software and data, helping with reproducing experiments of a published contribution. Some projects and publishers have also created repositories such as IEEE DataPort or Zenodo to create digital identifiers associated with the data submission. Behind these initiatives, an emerging trend is to enhance the management of the data, to increase the reusability by a third party [1]. This general principle, called the FAIR guiding principle, remains to be adapted for the particularity of data related to security.

This special issue desires to foster the progress in research on the scientific methodology of information security, in all aspects related to data, methods and guidelines that can help to replicate security experiments. In particular, we intend to improve the links between sub-domains of information security research and to propose to revisit existing research data and results by reproducing past experiments.

2 Articles of this special issue

This special issue covers extended articles of selected work presented during the *Third International Workshop on Information Security Methodology and Replication Studies* (IWSMR'21) workshop, co-located with the ARES'21 conference. Furthermore, articles from an open call on infor-

***Corresponding author: Steffen Wendzel,** Hochschule Worms, Zentrum für Technologie und Transfer – ZTT, D-67549 Worms, Germany, e-mail: wendzel@hs-worms.de
Luca Caviglione, National Research Council of Italy, Via de Marini 6, I-16149 Genova, Italy, e-mail: luca.caviglione@cnr.it
Aleksandra Mileva, Faculty of Computer Science, University "Goce Delcev", St. "Krste Misirkov" 10-A, Štip, Republic of N. Macedonia, e-mail: aleksandra.mileva@ugd.edu.mk
Jean-Francois Lalande, CentraleSupélec/Inria, IRISA, av. de la Boulaie, CS 47601 F-35576 Cesson-Sévigné, France, e-mail: jean-francois.lalande@irisa.fr
Wojciech Mazurczyk, Warsaw University of Technology, Nowowiejska 15/19, 00-665 Warsaw, Poland, e-mail: wojciech.mazurczyk@pw.edu.pl

mation security research methodology and replicability in cybersecurity were included in this special issue. Out of the ten submissions, three have finally been accepted for publication (acceptance rate: 33.3 %). Moreover, this special issue covers two distinguished dissertations.

The first two articles are extended versions of IWSMR'21 publications. Carina Heßeling and Jörg Keller study replicability challenges for chaotic pseudo random number generators. The authors discuss the uncertainties regarding the rounding mode in arithmetic hardware and propose a structured description in numerical experiments to address this issue.

Rafael Copstein, Egil Karlsen, Jeff Schwartzentruber, Nur Zincir-Heywood and Malcolm Heywood evaluate three feature extraction and three clustering methods (K-Means, DBSCAN and EM) on four security datasets for anomaly detection in the context of log abstraction.

One of the articles from the open call was also accepted. Aaron Weathersby and Mark Washington perform a replication study of an original article by Mireles et al. [2], in which the authors extracted attack narratives from individual cyber alerts within a network dataset. Weathersby et al. additionally extend this previous work by integrating suggestions of the original authors in their study.

The two accepted distinguished dissertation articles provide the following contributions. Guido Schmitz analyzes whether Single Sign-on (SSO) protocols used in the web actually meet their required security and privacy goals. His work has shown critical vulnerabilities in SSO protocols and provides remedies.

Finally, the work from Daniel Demmler shows how real-world applications of secure multi-party computation and private information retrieval can be executed in an efficient manner with realistic input sizes.

References

1. M. Wilkinson and M. Dumontier and I. Aalbersberg et al. *The FAIR Guiding Principles for scientific data management and stewardship*. Scientific Data 3, 2016.
2. J. D. Mireles and J. H. Cho and S. Xu. *Extracting attack narratives from traffic datasets*. Proc. 2016 International Conference on Cyber Conflict (CyCon US), IEEE, 2016.

Bionotes

Prof. Dr. Steffen Wendzel
Hochschule Worms, Zentrum für Technologie und Transfer – ZTT, D-67549 Worms, Germany
wendzel@hs-worms.de

Prof. Dr. Steffen Wendzel is a professor of information security and computer networks at Hochschule Worms, Germany, where he is also the scientific director of the Center for Technology and Transfer (ZTT). In addition, he is a lecturer at the Faculty of Mathematics & Computer Science at the FernUniversität in Hagen, Germany, from which he also received his Ph. D. (2013) and Habilitation (2020). Before joining Hochschule Worms, he led a smart building security research team at Fraunhofer FKIE in Bonn, Germany. Steffen (co-)authored more than 170 publications and (co-)organized several conferences and workshops (e. g., EICC'21, Sicherheit'16, IWSMR'19–'22) and special issues for major journals, such as IEEE Security & Privacy (S&P), Elsevier Future Generation Computer Systems (FGCS), Journal of Universal Computer Science (J. UCS), Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), and IEEE Transactions Industrial Informatics (TII). He is editorial board member of J. UCS, Journal of Cybersecurity & Mobility (JCSM) and Frontiers in Computer Science. His major research focus is on covert channels, network steganography, scientific taxonomy, and IoT security. Website: https://www.wendzel.de.

Dr. Luca Caviglione
National Research Council of Italy, Via de Marini 6, I-16149 Genova, Italy
luca.caviglione@cnr.it

Dr. Luca Caviglione is a Senior Research Scientist at the Institute for Applied Mathematics and Information Technologies of the National Research Council of Italy. He holds a Ph. D. in Electronic and Computer Engineering from the University of Genoa, Italy. His research interests include optimization of large-scale computing frameworks, traffic analysis, wireless and heterogeneous communication architectures, and network security. He is an author and co-author of more than 150 academic publications, and several patents in the field of p2p and energy-aware computing. He has been involved in Research Projects and Network of Excellences funded by the ESA, the EU and the MIUR. He is a work group leader of the Italian IPv6 Task Force, a contract professor in the field of networking/security and a professional engineer. He is the head of the IMATI Research Unit of the National Inter-University Consortium for Telecommunications and part of the Steering Committee of the Criminal Use of Information Hiding initiative.

Prof. Dr. Aleksandra Mileva
Faculty of Computer Science, University "Goce Delcev", St. "Krste Misirkov" 10-A, Štip, Republic of N. Macedonia
aleksandra.mileva@ugd.edu.mk

Prof. Dr. Aleksandra Mileva received the B. Sc., M. Sc., and Ph. D. degrees from Ss. Cyril and Methodius University in Skopje, Macedonia. She is currently a Full Professor with the Faculty of Computer Science, University Goce Delcev, Štip, Macedonia, where she is also the Head of the Laboratory of Computer Security and Computer Forensics. Her research interests include computer and network security, digital steganography, the IoT protocols and security, cryptography, computer forensics, and quasigroups theory. Since 2019, she has been a member of the EURASIP Data Forensics and Security TAC. She was with the management committee of two COST actions IC1201: BETTY and IC1306: Cryptography for Secure Digital Interaction. She is also member of the editorial boards of the Journal of Cyber Security and Mobility, and Mathematics, Computer Science and Education.

Prof. Dr. Jean-Francois Lalande
CentraleSupélec/Inria, IRISA, av. de la Boulaie, CS 47601 F-35576 Cesson-Sévigné, France
jean-francois.lalande@irisa.fr

Prof. Dr. Jean-Francois Lalande is Full Professor at CentraleSupélec. He is also part of the CIDRE team of Inria, in the IRISA laboratory. He received his Ph. D. degree in computer science from University of Nice Sophia-Antipolis, France. He was recruited as a permanent Associate Professor with the INSA Centre Val de Loire in 2005, in the LIFO laboratory. From September 2013 to August 2015, he moved to Inria (Rennes) as a delegated researcher and worked with the CIDRE team. In 2016, he obtained his habilitation to supervize research, from the University of Orléans. In 2019, he joined CentraleSupélec as Full Professor. His areas of interest are the security of operating systems, embedded software and mobile applications. He works on malware analysis, access control policies, intrusion detection tools and software code analysis. For the last 10 years, Jean-Francois Lalande co-authored more than 30 papers in journals, conferences, book chapters and workshops with international peer review and proceedings.

Prof. Dr. Wojciech Mazurczyk
Warsaw University of Technology, Nowowiejska 15/19, 00-665 Warsaw, Poland
wojciech.mazurczyk@pw.edu.pl

Prof. Dr. Wojciech Mazurczyk is a University Professor with Institute of Computer Science, Faculty of Electronics and Information Technology, Warsaw University of Technology (WUT), Poland. He received his B. Sc. (2003), M. Sc. (2004), Ph. D. (2009, with honours) and D. Sc. (habilitation, 2014) all in Telecommunications from WUT. He also is an author or co-author of 2 books, over 200 papers, 2 patent applications and over 35 invited talks. He has been involved in many international and domestic research projects as a principal investigator or as a senior researcher. He served as a guest editor of many special issues devoted to network security (among others: IEEE TDSC, IEEE S&P, IEEE Commag). He has been serving as Technical Program Committee Member of (among others): RAID, IEEE GLOBECOM, IEEE ICC, IEEE LCN, IEEE CNS, ACSAC, ARES and ACM IH&MMSec. From 2016 Editor-in-Chief of an open access Journal of Cyber Security and Mobility. Between 2018 and 2020 he was an Associate Editor of the IEEE TIFS and MCN Series Editor for the IEEE ComMag.