Guest Editorial: Multidisciplinary Solutions to Modern Cybersecurity Challenges

Luca Caviglione[1], Steffen Wendzel[2], Aleksandra Mileva[3], and Simon Vrhovec[4]
[1]Institute for Applied Mathematics and Information Technologies, Italy
[2]Hochschule Worms, Germany & FernUniversität in Hagen, Germany
[3]University "Goce Delcev", North Macedonia
[4]University of Maribor, Slovenia

Modern network and computing scenarios are characterized by a complex continuum spread across a variety of technological and administrative domains. For instance, cloud infrastructures are used to offload personal devices, IEEE 802.11 and 4G/5G connectivity allow ubiquitous mobility, and low-power communications and edge/fog computing enable to integrate cyber-physical systems in the daily routine. Moreover, software platforms are not characterized anymore by clear and precise technological and functional boundaries. In fact, modern smart services often span over multiple actors, e.g., product vendors, telcos, proprietary Software-as-a-Service deployments, as well as several nations (possibly with incompatible laws).

As a consequence, the Internet is a mixed collection of IoT devices, traditional hosts, wearable and mobile devices as well as individuals. Needles to say, its increasing human-centric nature accounts for a huge load of sensitive data, which can be considered one of the most valuable resource of our times. This mutation leads to an attack surface that is magnified by such a heterogeneity. To mention some potential issues, new reconnaissance techniques are discovered on a daily basis, and attacks/weaponization of threats targeting both the cyber and physical security of users can now take advantage of several exploitable features, such as those characterizing modern mobile smartphones.

In this perspective, assessing the cybersecurity of modern ICT platforms and frameworks requires a multi-/interdisciplinary effort, and the technological background must be completed with knowledge borrowed from different fields such as behavioral sciences, sociology, criminology, investigations and law. The *European Interdisciplinary Cybersecurity Conference* (EICC) is becoming one of the most important venues for the exchange of information on cybersecurity and where to present cutting-edge research on the sophisticated mix of technologies characterizing modern ICT services.

This Special Issue contains a selection composed of extended versions of the best papers presented at EICC 2020 and papers accepted from an "open call". In essence, the corpus of works deals with solutions, problems, defense mechanisms, forensics issues, threat analysis and development of countermeasures that leverage or require a multidisciplinary approach.

The first group of papers has been presented at EICC 2020 and clearly represents the multifaceted nature of modern cybersecurity challenges. In more detail, the work *ShadowHeap: Memory Safety through Efficient Heap Metadata Validation* proposes a new approach to prevent the run-time corruption of the heap, i.e., a copy of heap metadata is maintained to verify if operations can void the integrity of the memory. Such an advancement is important, especially if considering that stack smashing attacks and buffer overflows are the prime source of insecurity used to launch attacks on many devices. In general, upon compromised, devices/nodes/appliances are also the target of data exfiltration attempts (e.g., to

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), 12(4):1-3, Dec. 2021
DOI:*10.22667/JOWUA.2021.12.31.001*

feed phishing campaigns based on social engineering). Besides, the complex internetwork of services could be used to hide, via a needle-in-the-haystack approach, the coordination or orchestration of attacks (e.g., large-scale DDoS). Hence, being able to anticipate possible trends or assess the ability of de-facto standard security mechanisms to deal with network covert channels is vital. The work *Covert Channels in Transport Layer Security: Performance and Security Assessment* tries to enlighten the current situation of TLS-based conversations. Lastly, since humans are (and will always be) the most critical part of the security process, endowing them with a suitable background is a mandatory step. In this vein, the work *Enabling Exercises, Education and Research with a Comprehensive Cyber Range* discusses cutting-edge aspects in training, also with the use of tools like the cyber range.

The second group of papers has been accepted from an open call after a thorough review process. As hinted, devices are an important building block of modern ICT scenarios and also a huge source of insecurities. Luckily, machine learning can partially help in balancing the arm race between attackers and defenders. The work *Behaviour-based Malware Detection in Mobile Android Platforms Using Machine Learning Algorithms* gives a comprehensive view on the use of state-of-the-art techniques taking advantage of artificial intelligence when dealing with threats/misbehaviour of the widespread Android OS. Lastly, the increasing use of cloudification, containerization, virtualization, etc., requires to rethink tools used to inspect hardware/software platforms and to enforce network security. Indeed, networking and computing are progressively blending, thus accounting for a new multidisciplinary approach spanning across computer science and engineering. The work *An Effective and Efficient Approach to Improve Visibility Over Network Communications* showcases the use of the extended Berkeley Packet Filter to inspect network communications and enable the detection of a new-wave of threats.

As a concluding remark, we would like to thank the authors who submitted their work both to EICC and this Special Issue, as well as the reviewers who helped in the selection process. We also would like to thank the Editor in Chief for the support during the creation of this Special Issue.

Luca Caviglione, Steffen Wendzel, Aleksandra Mileva & Simon Vrhovec
Guest Editors
November 2021

Author Biography

Luca Caviglione is a Senior Research Scientist with the Institute for Applied Mathematics and Information Technologies of the National Research Council of Italy, Genoa. His research interests include optimization of large-scale computing frameworks, wireless and heterogeneous communication architectures, and network security. He is an author or 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 many research projects funded by the European Space Agency, the European Union, and the Italian Ministry of Research. 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. Contact him at luca.caviglione@cnr.it.

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. 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 160 publications and (co-)organized several conferences and workshops (e.g. EICC'21, Sicherheit'16, IWSMR'19, '20 and '21) 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 website: `https://www.wendzel.de`

Aleksandra Mileva is a full professor at Faculty of Computer Science, University Goce Delcev in Stip, Republic of N. Macedonia, where she is also the Head of the Laboratory of Computer Security and Digital Forensics. She received her PhD in Computer Science from the Ss. Cyril and Methodius University in Skopje in 2010. Her research interests include computer and network security, digital steganography, 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, and she is also a member of the editorial boards of the Journal of Cyber Security and Mobility, and the Mathematics, Computer Science and Education. She served as a guest editor for IEEE Internet of Things Journal, IEEE Security & Privacy, Journal of Universal Computer Science, etc. Contact her at aleksandra.mileva@ugd.edu.mk.

Simon Vrhovec is associate professor at the University of Maribor, Slovenia. He received his PhD degree in Computer and Information Science from the University of Ljubljana (Slovenia) in 2015. He is editorial board member of the Journal of Cyber Security and Mobility, Frontiers in Computer Science, EUREKA: Social and Humanities, and International Journal of Cyber Forensics and Advanced Threat Investigations (CFATI). He serves or has served as guest editor for IEEE Security & Privacy, Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), and Journal of Universal Computer Science (J.UCS). He is in the steering committee of the European Interdisciplinary Cybersecurity Conference (EICC) since 2019, and co-chaired the Central European Cybersecurity Conference (CECC) in 2018 and 2019. His main research interests are in human factors in cybersecurity, secure software development, agile methods, and change management. Contact him at simon.vrhovec@um.si.