Guest Editorial: Special Issue on Interdisciplinary Cybersecurity

Simon Vrhovec[1], Bela Genge[2], and Martin Gilje Jaatun[3]
[1]*University of Maribor, Slovenia*
[2]*"George Emil Palade" University of Medicine, Pharmacy, Science and Technology of Targu Mures Romania*
[3]*University of Stavanger, Norway*

Cyberspace has become a complex continuum spanning a variety of network technologies and domains, such as cloud, fog and edge infrastructures, and wired, wireless and mobile networks. It enables a ubiquitous interconnection of heterogeneous devices, such as traditional hosts; smart, internet of things (IoT), wearable, and mobile devices; as well as individuals and organizations. This results in pervasive collection and use of sensitive data.

Such a heterogeneous and sophisticated mix of technologies, devices and people inevitably poses significant challenges both for the security of connected devices and systems, and the privacy of individuals and organizations that they interact with, as new reconnaissance techniques and attacks are released on a daily basis. The situation for systems which include smart devices is further aggravated by a multitude of actors, such as manufacturers, service providers, app developers, telcos, and proprietary Software-as-a-Service (SaaS) deployments, in addition to the global nature of the cyberspace spanning over varying and potentially incompatible legislation.

Ensuring cybersecurity of modern systems therefore requires a strong technological foundation complemented by efforts stemming from other areas, 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 is composed of a selection of extended versions of the best papers presented at EICC 2021 and papers accepted from an open call. In essence, the corpus of works deals with solutions, problems, threat analysis and development of countermeasures that leverage or require an interdisciplinary approach to cybersecurity.

The first group of papers has been presented at EICC 2021 and clearly represents the multifaceted nature of modern cybersecurity challenges. The work *Anomaly Detection for Industrial Control Systems Through Totally Integrated Automation Portal Project History* proposes a novel approach for detecting mistakes done by employees and malicious manipulations by attackers or saboteurs who have gained access to the machines. The proposed approach combines heuristics with machine learning algorithms to detect timing- and size-based anomalies in the Totally Integrated Automation (TIA) Portal data. Detection of such anomalies is crucial to prevent attacks that can cause physical harm. For example, the proposed approach could help several noteworthy attacks in the past, such as *Stuxnet* (2010), *Havex* (2013), *Irongate* (2016), *Industroyer* (2017), *Triton* (2017) and possibly a series of explosions at the nuclear energy facilities in Iran (2020). The work *Improved Concept and Implementation of a Fountain Code Covert Channel* presents a multilevel method for network steganography within a fountain code as carrier. Fountain codes are used to provide reliable communication with low overhead over a lossy network, such as wireless sensor networks. New insights into such network steganography methods are

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), 13(3):1-3, Sept. 2022
DOI:*DOI: 10.22667/JOWUA.2022.09.30.001*

crucial for developing adequate countermeasures against various kinds of cyberattacks leveraging them (e.g., orchestration of DDoS attacks).

The second group of papers has been accepted from an open call after a thorough review process. The work *Hiding Data in a Switched Network* extends the works in the first group by proposing two new methods for covert channels in organizations using the three-tier hierarchical network model. This model is built of an access (i.e., hubs, bridges, switches and/or routers connected to end devices), distribution (i.e., mid-tier routers and switches) and core layers (i.e., high-end routers and switches that connect the distribution network devices between themselves and to outside services, such as the Internet), and heavily deploys the concept of Virtual Local Area Network (VLAN) as a logical group of hosts that belong to the same broadcast domain regardless of their physical location. The countermeasures presented in the paper are thus important to secure organizational networks against cyberattacks, such as data exfiltration attempts. The work *Detection of Steganographic Threats Targeting Digital Images in Heterogeneous Ecosystems Through Machine Learning* presents an ecosystem exploiting artificial intelligence techniques to reveal the presence of images embedding malicious assets. The proposed approach is an important countermeasure against malware built on an attack paradigm based on cloaking malicious payloads in innocent-looking pictures which are normally used by several devices and applications (e.g., to improve user experience). This attack paradigm is expected to become widely used in the near future due to the increasing popularity of application stores, availability of cross-platform services, and the adoption of various devices for entertainment and business duties. The work *Use of smart devices by the elderly: Nursing home residents in Slovenia* rounds up the interdisciplinary nature of cybersecurity by focusing on human aspects of the use of smart devices. It first identifies which smart devices are available to older adults and determines which of these devices are used by older adults in nursing homes. Next, it presents a preliminary analysis of exposure of older adults in nursing homes to cyberthreats due to their use of smart devices. These results are will gain in importance in the near- to mid-term future as smart devices get more widely used in nursing homes.

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 during peer review. We also would like to thank the Editor in Chief for the provided support during the creation of this Special Issue.

Simon Vrhovec, Bela Genge, and Martin Gilje Jaatun
Guest Editors
September 2022

Author Biography

Simon Vrhovec received the Ph.D. degree in computer and information science from the University of Ljubljana, Ljubljana, Slovenia, in 2015. He is currently an Associate Professor at the University of Maribor, Faculty of Criminal Justice and Security, Ljubljana, Slovenia. His main research interests include human factors in cybersecurity, software security engineering, agile methods, and change management. He has been 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. He is an Editorial Board Member of the Journal of Cyber Security and Mobility (JCSANDM), 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 a 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) (simon.vrhovec@um.si).

Bela Genge is a researcher at Bitdefender, and a professor at "George Emil Palade" University of Medicine, Pharmacy, Science and Technoogy of Tg. Mures. He received the Ph.D. degree in network security from the Technical University of Cluj-Napoca, Romania, in 2009. He has authored several papers in peer reviewed journals, including the International Journal of Critical Infrastructure Protection, IEEE Access, IEEE Transactions on Emerging Topics in Computing, IEEE Transactions on Smart Grid, and Future Generation Computer Systems. His research interests include security and resilience of networked control systems, and security in the Industrial Internet of Things. He has served as a TPC Member for several international events, including IEEE/IFIP Networking, ARES Workshops, and the European Interdisciplinary Cybersecurity Conference. He is a member of the Editorial Board of the International Journal of Critical Infrastructure Protection, Security and Communication Networks, and Journal of Cyber Security and Mobility.

Martin Gilje Jaatun is a Senior Scientist at SINTEF Digital in Trondheim, Norway. He graduated from the Norwegian Institute of Technology (NTH) in 1992, and received the Dr.Philos degree in critical information infrastructure security from the University of Stavanger in 2015. He is an adjunct professor at the University of Stavanger, and was Editor-in-Chief of the International Journal of Secure Software Engineering (IJSSE). Previous positions include scientist at the Norwegian Defence Research Establishment (FFI), and Senior Lecturer in information security at the Bodø Graduate School of Business. His research interests include software security, security in cloud computing, and security of critical information infrastructures. He is vice chairman of the Cloud Computing Association (cloudcom.org), vice chair of the IEEE Technical Committee on Cloud Computing (TCCLD), vice chair of the IEEE Computer Society Special Technical Community on Blockchain, an IEEE Cybersecurity Ambassador, an IEEE CS Distinguished Visitor, and a Senior Member of the IEEE.