Guest Editorial: Special Issue on the ARES-Workshops 2020

Peter Kieseberg and Simon Tjoa
JRC for Blockchain Technologies & Security Management
St. Pölten University of Applied Sciences
Matthias-Corvinus-Straße 15, 3100 St. Pölten

The ARES Workshops cover a wide variety of different topics in IT-Security, ranging from very technical approaches in digital forensics and malware detection to security management and threat intelligence. Thus, the Workshops serve as an integral part of ARES, not only due to the presentation of new results, but also with respect to the discussions initiated by presenting very recent result. Still, since the space reserved for workshop papers is limited, we decided to invite the best contributions to long-standing ARES workshops to submit extended versions. These journal versions as presented in this issue comprise fundamental extensions to the original works, as well as completely novel contributions based on the results of the original workshop papers and thus provide their own scientific merits rather than just being more elaborate versions of old results.

While IT-Security has become a wide field of expertise in the last decades, sporting many different sub-fields and requiring many different methods and tools, it is apparent that tools from the world of artificial intelligence gained a lot of attention throughout recent years, which is also reflected in the contributions in this special issue.

In order to react to attacks, detection is an especially important step. Thus, it is not surprising that three of the selected papers focus on issues surrounding detection, albeit focusing on different aspects and detection targets: Anomaly detection, detection of covert channels and identification of malware. In their paper *Machine Learning Based Approach to Anomaly and Cyberattack Detection in Streamed Network Traffic Data*, the authors extend their original approach and provided additional evaluations inside the SATIE network. The paper *Detecting Network Covert Channels using Machine Learning, Data Mining and Hierarchical Organisation of Frequent Sets* introduces the application of machine learning, as well as an error correction scheme, into the detection phase and removes some of the limitations inherent to the original approach. Similarly, in *Dynamic Mobile Malware Detection through System Call-based Image representation*, the original approach is substantially extended and refined.

The second part of the selected papers deals with managing systems security at large, providing different angles to this difficult and diverse problem. In the paper *Universal Identity and Access Management Framework for Future Ecosystems* the authors take the overview on differences and problems from the original work and build an approach for an Universal Identity and Access Management Framework. The work *Blockchain Mirage or Silver Bullet? A Requirements-driven Comparative Analysis of Business and Developers' Perceptions in the Accountancy* delivers a thorough extension of the original ARES Workshop paper and builds upon the original by providing a formal model. Last, but not least, the paper *Conflict Identification and Resolution for Trust-Related Requirements Elicitation - A Goal Modeling Approach* focuses on requirements engineering and extends the method for eliciting trust-related software features with the $i*$ goal modeling framework.

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications(JoWUA), 12(1):1-2, Mar. 2021
DOI:*10.22667/JOWUA.2021.03.31.001*

We would like to thank all authors that provided an extended version of their work to this special issue, as well as the workshop chairs that supported us and drove the selection of their top-submissions. We especially want to thank Prof. Ilsun You, Editor in Chief of JoWUA, for his intensive support throughout the preparation process of this special issue, as well as for providing the opportunity to publish it in JoWUA. Last, but not least, we want to thank Bettina Jaber from SBA Research to support us in the execution by contacting the authors and handling submissions.

Peter Kieseberg & Simon Tjoa
Guest Editors
March 2021

Author Biography

Peter Kieseberg heads the "Josef Ressel Center for Blockchain Technologies & Security Management", as well as the "Institute of IT Security Research" at the St. Pölten University of Applied Sciences, Austria, and has worked for more than 10 years in the field of IT Security Research. He is co-organizer of the Cross Domain Conference for Machine Learning and Knowledge Extraction (CD-MAKE) and founder and chair of the International Workshop on Security of Mobile Applications (IWSMA), which is taking place for the ninth time in 2020. Peter's research interests mainly focus on issues surrounding the foundations of blockchains regarding non-cryptocurrency applications, as well as privacy and data protection in data driven environments. He is a senior member of the IEEE and chair of the Austrian IEEE SMC chapter, as well as member of the ACM.

Simon Tjoa deputy head of the department "Computer Science and Security" at St. Pölten University of Applied Sciences and academic director of the master programs "Information Security" and "Cyber Security and Resilience". He received his doctoral degree in informatics from the University of Vienna and has been working for more than 15 years in the information security domain. He holds various information security certifications, such as Certified Information Systems Auditor (CISA) or Certified Information Security Manager(CISM). His research interests include cyber resilience, digital forensics and information security management. He currently researches on the interdependencies of Blockchain technologies and security management at the "Josef Ressel Center for Blockchain Technologies & Security Management". Furthermore, he serves as program committee member for several international conferences. He is a member of the IEEE and secretary of the Austrian IEEE SMC chapter.