Guest Editorial: Special Issue on the ARES-Workshops 2021

Peter Kieseberg and Simon Tjoa

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

In recent years, the ARES Workshops have emerged as important sources for ongoing research, covering 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. The Workshops have thus emerged to be an integral part of the ARES conference and provide a wide selection of novel results. Furthermore, the presentations given in these events drive discussions and new ideas, as well as new cooperations between partners, either inside a given field, but also across different areas if It Security. As the space reserved for workshop papers is limited and several contributions warranted a more in-depth discussion, 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. The reviewers, whom we want to thank very much, challenged these extensions for their scientific merits, thus guaranteeing the presence of valuable new results beyond pure extension on the presentation side.

The field of IT Security is sporting many different sub-fields, ranging from very technical topics to fields focusing on the human. The later has become especially important in recent years, with many attacks targeting the end user in order to either directly carry out the attack (e.g. in the case of CEO frauds), or to facilitate more technical attacks, e.g. by introducing highly specialized malware to systems secured by an air gap. This focus on the human is also reflected in the contributions in this special issue, reflecting developments in both, academia and industry, in recent years.

Thus, it is not surprising that three of the selected papers focus on issues around the end user, albeit focusing on different aspects: In their paper *SCADA Cybersecurity Awareness and Teaching with Hardware-In-The-Loop Platforms*, the authors present two twin demonstrators based on a common Hardware-In-the-Loop (HIL) technology, WonderICS, an Advanced Persistent Threat (APT) demonstrator used for awareness demonstrations, and G-ICS, a flexible lab used for students training and pentesting. Both approaches combine simulation, emulation and real devices to reproduce realistic industrial environments. The next paper *Architecture of a fake news detection system combining digital watermarking, signal processing, and machine learning* deals with the increasingly important topic of fake news detection, especially in the context of digital media, i.e. videos, images and audio, by proposing an architecture for a combined fake news detection system currently being developed within the DISSIMILAR project. The approach is a novel combination of digital watermarking, signal processing, and machine learning techniques. Focusing on the important topic of making security usable for end user, the work provided in *Empirical Validation on the Usability of Security Reports for Patching TLS Misconfigurations: User- and Case-Studies on Actionable Mitigations* presents a user study comparing two different

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), 13(1):1-3, Mar. 2022
DOI: *10.22667/JOWUA.2022.03.31.001*

approaches for reporting misconfigurations in TLS, including the design and lessons learned, thus focusing on making the utilization of automated tools more user centric and thus improve the development of secure software.

The second part of the selected papers deals with a selection of different topics highly relevant to the field of IT security. In the paper *Information Security Risks Analysis and Assessment in the Passenger-Autonomous Vehicle Interaction* the authors focus on the topic of protecting passenger data, as well as managing security risks in autonomous vehicles by presenting a novel approach for security risk management in the Passenger-AV interaction based on the domain model for information systems security risk management (ISSRM). Results include the identified protected assets and a threat model, as well as an approach for security risks and requirements assessment in order to enable the definition of a risk reduction strategy.

The work *Privacy-Preserving Analysis for Remote Video Anomaly Detection in Real Life Environments* also focuses on privacy, but in a completely different environment: While video surveillance is becoming increasingly important for safety and (non-IT) security, privacy is a primary concern. Thus, the paper proposes a new approach for privacy-preserving anomaly detection in surveillance video streams based on a supervised learning binary classification methodology, as well as providing an evaluation with a set of experiments on the UCF-CRIME video anomaly data set. Finally, the paper *Detection Of Computational Intensive Reversible Covert Channels Based On Packet Runtime* focuses on the detection of novel covert channels that rely on computationally expensive cryptographic primitives. Thus, the presented work approaches the problem by observing the influence of repeated MD5, SHA2-384, SHA3-256 and SHA3-512 hash-operations on packet runtimes through three experiments using different alphabets. In addition, the authors study detection capabilities of these novel computational intensive reversible covert channels and evaluate the detection rate based on the number of observed packets.

Finally, as guest editors 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 Daniela Freitag and Bettina Jaber from SBA Research, as well as Barbara Friedl from St. Pölten UAS to support us in the execution by contacting the authors and handling submissions. Last, but not least, a big shout-out to all the reviewers that did a great job in assessing the extended versions, thus making this special issue happen.

Peter Kieseberg & Simon Tjoa
Guest Editors
March 2022

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.