EURASIP Journal on Information Security

EDITORIAL Open Access

Cybersecurity: trends, issues, and challenges

Krzysztof Cabaj[1*], Zbigniew Kotulski[2], Bogdan Księżopolski[3] and Wojciech Mazurczyk[2]

In today's Internet-connected world where technologies underpin almost every facet of our society, cybersecurity and forensic specialists are increasingly dealing with wide ranging cyber threats in almost real-time conditions. The capability to detect, analyze, and defend against such threats in near real-time conditions is not possible without employment of threat intelligence, big data, and machine learning techniques. For example, when a significant amount of data is collected from or generated by different security monitoring solutions, intelligent and next-generation big-data analytical techniques are necessary to mine, interpret, and extract knowledge of these unstructured/structured (big) data. Thus, this gives rise to cyber threat intelligence and analytic solutions, such as big data, artificial intelligence, and machine learning, to perceive, reason, learn, and act against cyber adversary tactics, techniques, and procedures.

In this special issue, we are delighted to present a selection of six papers, which, in our opinion, will contribute to the enhancement of knowledge in cybersecurity. The collection of high-quality research papers provides a view on the latest research advances and results in the field of digital forensics and to present the development of tools and techniques which assist the investigation process of potentially illegal cyber activity. The fifth generation (5G) networks are still under construction, and their architecture is in a forming phase. There are several reports and white papers, especially these connected with the 5G Infrastructure Public Private Partnership (5G PPP), which attempt to precise 5G architectural requirements presenting them from different points of view, including techno-socio-economic aspects and technological constraints. All of them consider the network slicing as a central point, often strengthening slices with slice isolation.

The first paper "Towards constructive approach to end-to-end slice isolation in 5G networks" by Zbigniew Kotulski, Tomasz Wojciech Nowak, Mariusz Sepczuk, Marcin Tunia, Rafal Artych, Krzysztof Bocianiak, Tomasz Osko, and Jean-Philippe Wary [1] examines the isolation capabilities and selected approaches to its realization in network slicing context. As the 5G architecture is still evolving, the specification of isolated slice operation and management brings new requirements that need to be addressed, especially in a context of end-to-end (E2E) security. Its main purpose is presenting recent trends in slice isolation and a set of challenges faced in this field. These challenges could be a step from the concept of 5G networks to proof-of-concept solutions which provide E2E user's security based on slice isolation. According to authors' suggestions, the crucial features are proper slice design and establishment, security at interfaces, suitable access protocols, correct virtual resource sharing, and a dedicated adaptable management and orchestration architecture (MANO). Two main secure isolation challenges are presented in more details: a proper definition of isolation parameters and designing suitable MANO system.

The next article also focuses on 5G networks cybersecurity but from different perspective. The paper by Filipo Sharevski entitled "Towards 5G Cellular Network Forensics" [2] presents features of the 5G cellular networks which can be used during forensic process. At the first part of the paper, lawful interception (LI) and lawful access location service (LALS) mechanism of the LTE network are presented with details. These mechanisms, of course after obtaining a court warrant by the LEAs (Law Enforcing Agencies), allow access to the connections metadata, in the LTE called Interception Related Information (IRI), or even to the whole content of the communications. The second, most important part of the paper concerns how related functions can be implemented in the 5G network. Advantages of the 5G network are built using many techniques, to mentioned few, CUPS (Control and User Plane Separation), NFV (Network Functional Virtualization), network slicing, and CIoT (Cellular Internet-of-Things). These mechanisms are not developed with dedicated LI and LALS functionality, and

* Correspondence: kcabaj@ii.pw.edu.pl
[1]Institute of Computer Sciences, WUT, Nowowiejska 15/19, 00-665 Warsaw, Poland
Full list of author information is available at the end of the article

to enable it, some additional efforts are needed. The author of the paper presents some ideas and/or solution to overcome this problem. The paper is very infesting, as these mechanisms are seldom described and utilized by the researchers.

In the article entitled "Foundations and applications of artificial Intelligence for zero-day and multi-step attack detection authored" by Pierre Parrend, Julio Navarro, Fabio Guigou, Aline Deruyver, and Pierre Collet [3], another analysis of multi-step attack is presented. In this paper, the authors provide a review of the two main approaches for tracking hard-to-find cyberattacks: statistical analysis and machine learning, which are the two domains of data analysis. The authors propose a comprehensive framework for the study of complex attacks and related analysis strategies through statistical tools, on the one side, and machine learning tools, one the other side. It puts these complex attacks in perspective with their core applications in the security domain: detection and investigation. Transaction traces analysis is a key utility for marketing, trend monitoring, and fraud detection purposes. A good source of such traces are Points-of-Sale (POS) which are devices representing the transactions' checkout processes.

The data obtained from the traces is an effective source of information about shoppers, their purchases, and behaviors. The transaction traces can also be used for designing and verification of contextual risk management systems for card-present transactions.

In the paper "POS-originated transaction traces as a source of contextual information for risk management systems in EFT transactions" by Albert Sitek and Zbigniew Kotulski [4], the authors have presented a novel approach to collect detailed transaction traces directly from payment terminals. Thanks to that, it is possible to analyze each transaction's step precisely, including its frequency and timing. The authors have used such an approach to analyze the collected data based on real-life experiment. They also presented important findings for designers of such payment systems to extend their functionalities.

The next paper is entitled "OMMA: open architecture for Operator-guided Monitoring of Multi-step Attacks" authored by Julio Navarro, Veronique Legrand, Aline Deruyver, and Pierre Parrend [5]. The authors propose the architecture of an engineering system called OMMA, Operator-guided Monitoring of Multi-step Attacks, for integration of multi-step attack detection methods working with heterogeneous sets of events. OMMA proposes a framework for merging different detection techniques in order to improve research collaborations and profit from past work. The main contribution of OMMA is that it offers to the research community an open platform where no matter which multi-step attack detection algorithm based on event correlation could be integrated.

Finally, the paper "Detection of Spoofed and Non-Spoofed DDoS Attacks and Discriminating them from Flash Crowds" by Gera Jaideep and Bhanu Prakash Battula [6] focuses on introducing a novel methodology that is able to detect different types of DDoS attacks. Moreover, the proposed solution is able to differentiate such attacks from the benign flash crowd effect (which currently is perceived as a very challenging task). The presented comprehensive methodology takes into account various network traffic dynamic parameters like source entropy and traffic entropy and investigates different thresholds in order to be capable of correctly recognizing spoofed and non-spoofed DDoS attacks and flash crowd scenario. To prove that their solution is effective and efficient, the authors provide in the paper also extensive results of experiments conducted with the use of NS-2 simulator.

To summarize, we believe that this special issue will contribute to enhancing knowledge in cybersecurity. In addition, we also hope that the presented results will stimulate further research in the important areas of information and network security. We also want to thank the Editors-in-Chief of the *EURASIP Journal on Information Security*, the researchers contributing to the special issue, and excellent reviewers for their great help and support that made this special issue possible.

Authors' contributions

All authors actively participated in discussions, read and approved the final manuscript. All authors read and approved the final manuscript.

Competing interests

The authors declare that they have no competing interests.

Publisher's Note

Author details

[1]Institute of Computer Sciences, WUT, Nowowiejska 15/19, 00-665 Warsaw, Poland. [2]Institute of Telecommunications, WUT, Nowowiejska 15/19, 00-665 Warsaw, Poland. [3]Faculty of Mathematics, Physics and Computer Science, UMCS, pl. Marii Curie-Sk lodowskiej 5, 20-031 Lublin, Poland.

Received: 11 July 2018 Accepted: 12 July 2018
Published online: 20 July 2018

References

1. Z Kotulski, T.W Nowak, M Sepczuk, M Tunia, R Artych, K Bocianiak, T Osko and J-P Wary (2018). Towards constructive approach to end-to-end slice isolation in 5G networks. *EURASIP Journal on Information Security, 2018*, 2, Published on: 20 March 2018 https://doi.org/10.1186/s13635-018-0072-0 .
2. F Sharevski (2018). Towards 5G cellular network forensics. *Eurasip Journal on Information Security, 2018*, 8, Published on: 11 July 2018 https://doi.org/10.1186/s13635-018-0078-7 .
3. P Parrend, J Navarro, F Guigou, A Deruyver and P Collet (2018). Foundations and applications of artificial intelligence for zero-day and multi-step attack detection. *EURASIP Journal on Information Security 2018*,4, Published on: 24 April 2018 https://doi.org/10.1186/s13635-018-0074-y.

4. A Sitek and Z Kotulski (2018). POS-originated transaction traces as a source of contextual information for risk management systems in EFT transactions. *EURASIP Journal on Information Security 2018*,5, Published on: 27 April 2018 https://doi.org/10.1186/s13635-018-0076-9.
5. J Navarro, V Legrand, A Deruyver and P Parrend (2018). OMMA: open architecture for operator-guided monitoring of multi-step attacks. *Eurasip Journal on Information Security, 2018*,6. Published on: 2 May 2018 https://doi.org/10.1186/s13635-018-0075-x.
6. G Jaideep and B.P Battula (2018). Detection of spoofed and non-spoofed DDoS attacks and discriminating them from flash crowds. *Eurasip Journal on Information Security, 2018*:9. Published on: 16 July 2018 https://doi.org/10.1186/s13635-018-0079-6.