information

Editorial

Editorial for Special Issue Detecting Attack and Incident Zone System

Christoforos Ntantogian

Department of Informatics, Ionian University, 491 00 Corfu, Greece; dadoyan@ionio.gr

Attackers who have a strong motivation to succeed in their nefarious goals are often able to breach the security of their targets and cause havoc. On the other hand, defenders have proactive and reactive security mechanisms at their disposal, designed to withstand against such malicious actions. In the proactive security approach, each element of the information system, from software to hardware and from network devices to human activities, must be periodically tested to pinpoint security loopholes that must be patched up before any attacker tries to exploit them. Proactive security is not a panacea as it seems that there is always another security bug to fix. As such, reactive security measures are put in place to detect as soon as possible any successful attack before insurmountable damage occurs. By complementing each other, proactive and reactive security measures can significantly improve the security posture of systems and networks.

Let us place in this context the papers of this Special Issue, which were accepted, after a careful peer-review process, for publication in the Special Issue, "Detecting Attack and Incident Zone System", for the MDPI journal, *Information*. Proactive security approaches were proposed in the following three papers of the Special Issue.

"P2ISE: Preserving Project Integrity in CI/CD Based on Secure Elements" [1] identifies and analyzes the security gap that exists in the continuous integration and development pipeline regarding a software project's integrity. It proposes the design and implementation of P2ISE, a novel tool that employs TPM-trusted computing technology, which offers security assertions for code integrity, as well as to preventing unauthorized access.

"PocketCTF: A Fully Featured Approach for Hosting Portable Attack and Defense Cybersecurity Exercises" [2] is another work in favor of proactive security. It proposes an extensible and fully independent CTF platform, open to educators to run realistic virtual laboratories to host cybersecurity exercises. A proof-of-concept implementation demonstrates the feasibility of deploying CTF challenges that allow trainees to engage, not only in offensive security, but also in defensive tasks that are conducted during cybersecurity incidents.

"Compatibility of a Security Policy for a Cloud-Based Healthcare System with the EU General Data Protection Regulation (GDPR)" [3] focuses on the GDPR regulations that can significantly fortify the security of organizations. The major concept of this paper is dual-purpose: firstly, to facilitate cloud providers in comprehending the framework of the new GDPR, and secondly, to identify security measures and security policy rules for the protection of sensitive data in a cloud-based healthcare system.

Regarding reactive security, this Special Issue includes two papers. The work in [4], "A Comprehensive Survey on Machine Learning Techniques for Android Malware Detection", is a review paper that schematizes contemporary machine learning-based mobile malware detection techniques by organizing them under four axes: the age of the selected dataset, the analysis type used, the employed techniques, and the chosen performance metrics. Moreover, based on these axes, the paper introduces a converging scheme which can guide future Android malware detection techniques and provide a solid baseline for machine learning practices in this field.

check for updates

Citation: Ntantogian, C. Editorial for Special Issue Detecting Attack and Incident Zone System. *Information* **2021**, *12*, 382. https://doi.org/10.3390/info12090382

Received: 17 September 2021
Accepted: 17 September 2021
Published: 18 September 2021

Finally, the paper "SDToW: A Slowloris Detecting Tool for WMNs" [5] presents a tool that detects and blocks an application denial of service attacks on wireless mesh networks, called Slowloris. The performance valuation of the proposed tool provides not only its detection capabilities but also low false positive errors compared to intrusion detection solutions.

References

1. Muñoz, A.; Farao, A.; Correia, J.R.C.; Xenakis, C. P2ISE: Preserving Project Integrity in CI/CD Based on Secure Elements. *Information* **2021**, *12*, 357. [CrossRef]
2. Karagiannis, S.; Ntantogian, C.; Magkos, E.; Ribeiro, L.L.; Campos, L. PocketCTF: A Fully Featured Approach for Hosting Portable Attack and Defense Cybersecurity Exercises. *Information* **2021**, *12*, 318. [CrossRef]
3. Georgiou, D.; Lambrinoudakis, C. Compatibility of a Security Policy for a Cloud-Based Healthcare System with the EU General Data Protection Regulation (GDPR). *Information* **2020**, *11*, 586. [CrossRef]
4. Kouliaridis, V.; Kambourakis, G. A Comprehensive Survey on Machine Learning Techniques for Android Malware Detection. *Information* **2021**, *12*, 185. [CrossRef]
5. Faria, V.d.S.; Gonçalves, J.A.; Silva, C.A.M.d.; Vieira, G.d.B.; Mascarenhas, D.M. SDToW: A Slowloris Detecting Tool for WMNs. *Information* **2020**, *11*, 544. [CrossRef]