electronics

MDPI

Editorial

Advanced Cybersecurity Services Design

Victor A. Villagrá

Departamento Ingeniería Telemática (DIT), ETSI Telecomunicación (ETSIT), Universidad Politécnica de Madrid (UPM), Avda. Complutense 30, 28040 Madrid, Spain; victor.villagra@upm.es

1. Introduction

Cybersecurity technologies have been researched extensively in the last few years in order to face the current threat landscape, which has shown a continuous growth in the quality and quantity of attacks that are oriented toward any potentially vulnerable items (people, software, firmware, hardware, etc.). Thus, there is a need for more sophisticated cybersecurity services that are able to combine different technologies to cover all the different aspects that such attacks may utilize.

These advanced cybersecurity services must enrich the different areas of cybersecurity, including cyberattacks prevention, detection and response, as well as advanced supporting infrastructures for these services. Nowadays, most of the prevention initiatives rely on increasing users' awareness, in order to prevent social engineering attacks, but there are also some technological areas that can complement a security architecture for the prevention of cyberattacks. In the area of attacks detection, machine learning-based algorithms are one of the most promising techniques for anomaly detection, as well as the use of Cyber Threats Intelligence in order to share knowledge about the attacks. In the area of supporting infrastructure, there is an increasing interest in leveraging traditional cryptographic algorithms with new approaches, such as homomorphic encryption when privacy is concerned, quantum and post-quantum cryptography, and the use of blockchain technologies for different advanced cybersecurity services.

2. The Present Issue

This Special Issue includes 14 contributions that cover these areas. It includes two review contributions: [1] provides a survey with an overview of the state of the art in detecting and projecting cyberattack scenarios, i.e., approaches that automate the analysis of alerts to detect large-scale attacks and predict the attacker's next steps, with a focus on evaluation and the corresponding metrics. On the other hand, [2] reviews a specific application area, namely the identification and discussion of the relation between the safety of Autonomous Haulage Systems in the mining environment and both cybersecurity and communication; furthermore, the article highlights their challenges and open issues.

The Special Issue also includes 12 research contributions. It includes several contributions related to advanced services for Intrusion Detection Systems. In [3], the use of different machine learning models depending on the specific scenarios and datasets is addressed, as well as the design of an automatic dynamic model selector for anomalies detections scenarios. The article in [4] focuses on the use of deep learning techniques for the detection of zero-day attacks, with an autoencoder implementation that is able to monitor the rate of false-negative detection rates. In [5], an integrated scalable framework is proposed that aims at efficiently detecting anomalous events on large amounts of unlabelled data logs. Detection is supported by clustering and classification methods that take advantage of parallel computing environments using two models: one based on K-Means and the other based on a XGBoost system implementing a gradient tree boosting algorithm. In [6] a spatiotemporal characterization of cyberattacks for detecting cyberattacks is proposed

check for updates

Citation: Villagrá, V.A. Advanced Cybersecurity Services Design. *Electronics* **2022**, *11*, 2803. https://doi.org/10.3390/electronics11182803

Received: 1 September 2022
Accepted: 3 September 2022
Published: 6 September 2022

using a stochastic graph model to represent these cyberattacks in time and space. In [7], the area of industrial control networks is addressed with a two-stage intrusion detection system, including a traffic prediction model and an anomaly detection model. A chatbot is proposed in [8] for detecting online sex offenders, based on an Artificial Conversational Entity (ACE) that connects to different online chat services to start a conversation. The ACE was designed using generative and rule-based models in charge of generating the posts and replies that constitute the conversation from the chatbot side. The proposed solution also includes a module to analyse the conversations performed by the chatbot and calculate a set of 25 features that describes the suspect's behaviour. Finally, [9] introduces Insight2, an open-source platform for manipulating both streaming and archived network flow data in real time in order to understand normal activity and identify abnormal activity.

This Special Issue also contains two protection-related research contributions: [10] proposes a countermeasure for on-off web defacement attacks with a random monitoring strategy, designing and validating two specific strategies for such a purpose. On the other hand, [11] addressed the evaluation of multi-path routing as a protection feature against network attacks and failures, with the study of the following two different models: first-hop multi-path and multi-hop multi-path routing.

The Special Issue also includes several contributions about related technologies for providing support to the design of advanced cybersecurity services: [12] provides an analysis of a partially homomorphic encryption algorithm for the design of services needing privacy-preserving functionalities. In [13] a system for using blockchain technologies for the accountability of cybersecurity audit results is proposed in order to boost the automation of both digital evidence gathering, auditing, and controlled information exchange. The study in [14] focuses on the area of Cyber-Threat Intelligence Sources, and Formats and Languages, while investigating the landscape of the available formats and languages, along with the publicly available sources of threat feeds, how these are implemented and their suitability for providing rich cyber-threat intelligence.

3. Future Directions

Cybersecurity is nowadays a race between the attackers and the different digital technologies actors (users, manufacturers, IT companies, etc.). A new technology, or a new protection system is usually followed by a new attacker method, so there is a need for new services based on new technologies that might make possible the establishment of a gap with attackers, increasing the confidence on the usage of business and personal services by users. Therefore, there is a need to extend the research on these areas with the adequate support of public and private entities in order to generate new research proposals that might be able to find the different steps to establish a gap with the attackers. The proposals in this Special Issue might provide small steps in pursuit of this aim, but there is a need for many more initiatives to be designed, tested and validated in order to make secure technologies available for everybody.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: First of all, I would like to thank all the researchers who submitted articles to this Special Issue for their excellent contributions. I am also grateful to all the reviewers who helped in the evaluation of the manuscripts and made very valuable suggestions to improve the quality of the contributions. I would like to acknowledge the editorial board of *Electronics*, who invited me to guest edit this Special Issue. I am also grateful to the *Electronics* Editorial Office staff who worked thoroughly to maintain the rigorous peer-review schedule and timely publication.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Kovačević, I.; Groš, S.; Slovenec, K. Systematic Review and Quantitative Comparison of Cyberattack Scenario Detection and Projection. *Electronics* **2020**, *9*, 1722. [CrossRef]
2. Gaber, T.; El Jazouli, Y.; Eldesouky, E.; Ali, A. Autonomous Haulage Systems in the Mining Industry: Cybersecurity, Communication and Safety Issues and Challenges. *Electronics* **2021**, *10*, 1357. [CrossRef]
3. Larriva-Novo, X.; Sánchez-Zas, C.; Villagrá, V.; Vega-Barbas, M.; Rivera, D. An Approach for the Application of a Dynamic Multi-Class Classifier for Network Intrusion Detection Systems. *Electronics* **2020**, *9*, 1759. [CrossRef]
4. Hindy, H.; Atkinson, R.; Tachtatzis, C.; Colin, J.; Bayne, E.; Bellekens, X. Utilising Deep Learning Techniques for Effective Zero-Day Attack Detection. *Electronics* **2020**, *9*, 1684. [CrossRef]
5. Henriques, J.; Caldeira, F.; Cruz, T.; Simões, P. Combining K-Means and XGBoost Models for Anomaly Detection Using Log Datasets. *Electronics* **2020**, *9*, 1164. [CrossRef]
6. Kim, J.; Kim, H. Intrusion Detection Based on Spatiotemporal Characterization of Cyberattacks. *Electronics* **2020**, *9*, 460. [CrossRef]
7. Yu, W.; Wang, Y.; Song, L. A Two Stage Intrusion Detection System for Industrial Control Networks Based on Ethernet/IP. *Electronics* **2019**, *8*, 1545. [CrossRef]
8. Rodríguez, J.; Durán, S.; Díaz-López, D.; Pastor-Galindo, J.; Mármol, F. C3-Sex: A Conversational Agent to Detect Online Sex Offenders. *Electronics* **2020**, *9*, 1779. [CrossRef]
9. Kodituwakku, H.; Keller, A.; Gregor, J. InSight2: A Modular Visual Analysis Platform for Network Situational Awareness in Large-Scale Networks. *Electronics* **2020**, *9*, 1747. [CrossRef]
10. Cho, Y. Intelligent On-Off Web Defacement Attacks and Random Monitoring-Based Detection Algorithms. *Electronics* **2019**, *8*, 1338. [CrossRef]
11. An, H.; Na, Y.; Lee, H.; Perrig, A. Resilience Evaluation of Multi-Path Routing against Network Attacks and Failures. *Electronics* **2021**, *10*, 1240. [CrossRef]
12. Catak, F.; Aydin, I.; Elezaj, O.; Yildirim-Yayilgan, S. Practical Implementation of Privacy Preserving Clustering Methods Using a Partially Homomorphic Encryption Algorithm. *Electronics* **2020**, *9*, 229. [CrossRef]
13. Marín-López, A.; Chica-Manjarrez, S.; Arroyo, D.; Almenares-Mendoza, F.; Díaz-Sánchez, D. Security Information Sharing in Smart Grids: Persisting Security Audits to the Blockchain. *Electronics* **2020**, *9*, 1865. [CrossRef]
14. Ramsdale, A.; Shiaeles, S.; Kolokotronis, N. A Comparative Analysis of Cyber-Threat Intelligence Sources, Formats and Languages. *Electronics* **2020**, *9*, 824. [CrossRef]