algorithms

MDPI

Editorial

Special Issue "AI for Cybersecurity: Robust Models for Authentication, Threat and Anomaly Detection"

Francesco Bergadano [1,*] and Giorgio Giacinto [2]

[1] Department of Computer Science, University of Torino, Via Pessinetto 12, 10149 Torino, Italy
[2] Department of Electrical and Electronic Engineering, University of Cagliari, Piazza d'Armi, 09123 Cagliari, Italy; giacinto@unica.it
* Correspondence: francesco.bergadano@unito.it

1. Introduction

Cybersecurity models include provisions for legitimate user and agent authentication, as well as algorithms for detecting external threats, such as intruders and malicious software. In particular, we can define a continuum of cybersecurity measures ranging from user identification to risk-based and multilevel authentication, complex application and network monitoring, and anomaly detection. We refer to this as the "anomaly detection continuum".

Machine learning and other artificial intelligence technologies can provide powerful tools for addressing such issues, but the robustness of the obtained models is often ignored or underestimated. On the one hand, AI-based algorithms can be replicated by malicious opponents, and attacks can be devised so that they will not be detected (evasion attacks). On the other hand, data and system contexts can be modified by attackers to influence the countermeasures obtained from machine learning and render them ineffective (active data poisoning).

This Special Issue presents ten papers [1–10] that can be grouped under five main topics.

2. Cyber Physical Systems (CPSs) [1–3]

AI techniques are particularly needed for the security of CPSs. This is due to the high number and large variety of devices that cannot be manually controlled and monitored. Security automation is also needed in this context because of the deployment of the target infrastructure, which is often remote and difficult to access physically. The first paper [1] reviews existing studies and datasets for anomaly detection in CPSs. In [2], the authors propose a new approach for multi-vector attack detection in the IoT domain, using machine learning algorithms and providing an experimental evaluation. In article [3], classifiers obtained via machine learning were applied to the security monitoring of smart grids, and an adaptive deep learning algorithm is proposed and evaluated with the NSL-KDD dataset.

3. Intrusion Detection [4,5]

Intrusion detection is traditionally a common target of AI applications in the context of cybersecurity because machine learning can provide a means to train models that distinguish normal traffic from malicious attacks. The fourth paper [4] studies such issues in the particular context of cooperative intelligent transportation systems, proposing algorithms and an intrusion detection architecture evaluated on the NGSIM dataset. The fifth paper [5] is devoted to network intrusion detection and addresses the problems of high false negative rates and low predictability for minority classes.

4. Malware Analysis [6]

Malware detection, analysis, and response can be partly automated with artificial intelligence. The number and variety of malware attacks make this a necessity, as manual inspection, as well as ad hoc countermeasures, would be impossible. In [6], the authors

Citation: Bergadano, F.; Giacinto, G. Special Issue "AI for Cybersecurity: Robust Models for Authentication, Threat and Anomaly Detection". *Algorithms* **2023**, *16*, 327. https://doi.org/10.3390/a16070327

Received: 29 June 2023
Accepted: 30 June 2023
Published: 7 July 2023

compare different ensemble learning methods that have been proposed in this context: Random Forests, XGBoost, CatBoost, GBM, and LightGBM. Experiments were performed on different datasets, finding that tree-based ensemble learning algorithms can achieve good performance with limited variability.

5. Access Control [7,8]

As stated above, access control can be viewed as another point in the anomaly detection continuum. Again, distinguishing a legitimate user from impostors can be automated through machine learning. The seventh paper [7] addresses this in the context of face recognition systems (FRSs) and proposes a practical white box adversarial attack algorithm. The method is evaluated with the CASIA WebFace and the LFW datasets. In [8], the authors used the legitimate user's iris image, combined with a secret key, to generate a public key and subsequently use such data to limit access to protected resources.

6. Threat Intelligence [9,10]

Not only do we want to recognize and block attacks as they occur—we also need to observe external data and the overall network context to predict relevant events and new attack patterns, addressing the so-called threat intelligence landscape. In [9], the authors used two well-known threat databases (CVE and MITRE) and proposed a technique to link and correlate these two sources. The tenth paper [10] used formal ontologies to monitor new threats and identify the corresponding risks in an automated way.

7. Conclusions

In conclusion, we observed that AI is increasingly being used in cybersecurity, with three main directions of current research: (1) new areas of cybersecurity are addressed, such as CPS security and threat intelligence; (2) more stable and consistent results are being presented, sometimes with surprising accuracy and effectiveness; and (3) the presence of an AI-aware adversary is recognized and analyzed, producing more robust and reliable solutions.

Author Contributions: Special issue editorial by both authors. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Tushkanova, O.; Levshun, D.; Branitskiy, A.; Fedorchenko, E.; Novikova, E.; Kotenko, I. Detection of Cyberattacks and Anomalies in Cyber-Physical Systems: Approaches, Data Sources, Evaluation. *Algorithms* **2023**, *16*, 85. [CrossRef]
2. Lysenko, S.; Bobrovnikova, K.; Kharchenko, V.; Savenko, O. IoT Multi-Vector Cyberattack Detection Based on Machine Learning Algorithms: Traffic Features Analysis, Experiments, and Efficiency. *Algorithms* **2022**, *15*, 239. [CrossRef]
3. Li, X.J.; Ma, M.; Sun, Y. An Adaptive Deep Learning Neural Network Model to Enhance Machine-Learning-Based Classifiers for Intrusion Detection in Smart Grids. *Algorithms* **2023**, *16*, 288. [CrossRef]
4. Almalki, S.A.; Abdel-Rahim, A.; Sheldon, F.T. Adaptive IDS for Cooperative Intelligent Transportation Systems Using Deep Belief Networks. *Algorithms* **2022**, *15*, 251. [CrossRef]
5. Mijalkovic, J.; Spognardi, A. Reducing the False Negative Rate in Deep Learning Based Network Intrusion Detection Systems. *Algorithms* **2022**, *15*, 258. [CrossRef]
6. Louk, M.H.L.; Tama, B.A. Tree-Based Classifier Ensembles for PE Malware Analysis: A Performance Revisit. *Algorithms* **2022**, *15*, 332. [CrossRef]
7. Lang, D.; Chen, D.; Huang, J.; Li, S. A Momentum-Based Local Face Adversarial Example Generation Algorithm. *Algorithms* **2022**, *15*, 465. [CrossRef]
8. Matveev, I.; Safonov, I. From Iris Image to Embedded Code: System of Methods. *Algorithms* **2023**, *16*, 87. [CrossRef]

9. Grigorescu, O.; Nica, A.; Dascalu, M.; Rughinis, R. CVE2ATT&CK: BERT-Based Mapping of CVEs to MITRE ATT&CK Techniques. *Algorithms* **2022**, *15*, 314.
10. Shaked, A.; Margalit, O. Sustainable Risk Identification Using Formal Ontologies. *Algorithms* **2022**, *15*, 316. [CrossRef]