applied sciences

MDPI

Editorial

Advances in Cybersecurity: Challenges and Solutions

Peter R. J. Trim [1,*] and Yang-Im Lee [2,*]

[1] Birkbeck Business School, Birkbeck, University of London, Malet Street, London WC1E 7HX, UK
[2] Westminster Business School, University of Westminster, 35 Marylebone Road, London NW1 5LS, UK
* Correspondence: p.trim@bbk.ac.uk (P.R.J.T.); y.lee@westminster.ac.uk (Y.-I.L.)

1. Introduction

Cyberattacks have increased in intensity and sophistication in recent years, resulting in defensive actions to safeguard company assets and vulnerable people. Research undertaken into various forms of cyberattacks has introduced a number of methods and approaches to help counteract the actions of those responsible for attacks of this nature [1]. However, fully understanding the factors involved requires an in-depth appreciation of the type of attack and the possible impact on an organization should it be successful in penetrating the organization's defences. Indeed, as change occurs in society and people adapt accordingly, new vulnerabilities emerge. For example, although remote working is perceived as beneficial from a cost effectiveness perspective, it can be argued that the benefits afforded to employees, which include the opportunity to work flexibly and utilize their own personal device(s) to access organizational computer systems when working from home, need to be weighed against the possible risks involved. It must be highlighted that the Bring Your Own Device (BYOD) model [2] can put both the employee and the organization at risk if the employee does not follow the security guidance provided. Hence, monitoring and organizational control are important factors in terms of ensuring that the use of a personal device does not prove problematic.

With the advances in artificial intelligence (AI) and the anticipated advantages and threats associated with it, it is pleasing to note that work that is being carried out to ensure that networking platforms are safer, is focused on making networks more robust. Studies relating to data-driven edge intelligence vis-à-vis robust network anomaly detection will contribute significantly to making data secure, and the benefits associated with network anomaly detection [3] will help security provision. The evolving nature of cyber threats has resulted in various initiatives involving corporate, government and academic researchers, all of whom have contributed to the defence of society. In the process, cooperation involving institutions and cybersecurity experts, has witnessed cross border initiatives that have helped preserve the quality of life. Future technological collaboration and knowledge transfer between cybersecurity researchers will do much to speed up the process of developing new technological solutions to combat innovative practices emanating from cyber criminals.

Cyberattacks have an international dimension; as such, cybersecurity researchers need to find ways to collaborate, which requires clear leadership. However, although new technologies are emerging and being approved and are partially funded by the government, smart cities will be at risk if the technologies that underpin critical infrastructure are deficient. It has been suggested [4] that attention needs to be paid to SCADA systems, and in particular power grid subsystems. With cybersecurity threat detection remaining high on the agenda of cybersecurity researchers and senior managers, it can be expected that more attention will be given to establishing how the Internet of Things (IoT) will be prone to malware attacks [5]. Much is known about such attacks, but the perpetrators of such attacks are increasingly seeking to exploit new vulnerabilities and will continue to do so for a considerable time. Whether their motivation is associated with financial gain or attributed to a desire to cause disruption and gain publicity is of interest to cybersecurity researchers.

check for updates

Citation: Trim, P.R.J.; Lee, Y.-I. Advances in Cybersecurity: Challenges and Solutions. *Appl. Sci.* **2024**, *14*, 4300. https://doi.org/10.3390/app14104300

Received: 30 April 2024
Accepted: 17 May 2024
Published: 19 May 2024

Clearly, international cooperation to counteract the actions of cyber criminals and threat agents will continue to be the focus of policy makers, highlighting the importance of identifying solutions to recurring threats. Acknowledging that cybersecurity needs to be properly managed and resourced focuses attention on various research initiatives, both present and evolving, that will help identify solutions and make organizations less vulnerable to attacks. Therefore, building a practical environment in which cybersecurity training and weapon system test evaluations [6] can be undertaken is essential. Acknowledging that cybercrime is also associated with acts of cyber war and cyber terrorism, provides policy makers with the grounds to regulate more widely to prevent the evolution of more advanced forms of cyberattacks. Advances in artificial intelligence (AI) will be a game changer and require more investment in order to better understand how to defend against AI-orchestrated attacks. However, the advances made in technology will not distract from the fact that managers in both the public and private sectors need to ensure that staff are compliant and comply with security practices [7]. To ensure that this happens, appropriate governance framework(s) and mechanism(s) need to be put in place.

To solve the underlying root of recurring cybersecurity threats and issues, cybersecurity researchers need to implement cybersecurity policy and strategy initiatives that will help counteract the effort of those intent on destabilizing society and causing untold damage for their own gain. Hence, this Special Issue is dedicated to developments in cybersecurity from an interdisciplinary and multidisciplinary perspective, and the collection of papers focus on the challenges confronting companies, governments and society. The topics covered establish the ways in which technology and human–technology interactions are enhancing cybersecurity provision. By adopting a holistic view of cybersecurity and outlining the strategies to implement cybersecurity solutions, it is possible for society to be better-protected and more able to withstand sustained cyberattacks. A broad range of papers are included in the Special Issue, and various methodological approaches are represented that help us understand how cybersecurity theory and practice are linked and how we can devise and implement effective cybersecurity solutions.

2. An Overview of the Published Articles

The range of topics covered and knowledge accumulated by the authors can be considered inspirational, setting the scene for future research into cyber security and the related areas of study. Indeed, Ayedh et al. pay attention to an important but under-researched topic, Bring Your Own Device (BYOD), referring to the relevant security and privacy requirements. As well as covering BYOD security policies, reference is made to state-of-the art security policy technologies, technology trends and the measures employed to enhance security.

Another area of increased attention is the need for maintaining a secure system by acquiring necessary learning data. In their paper, Cha et al. make reference to a digital twin environment and focus on the need to ensure that systems and data in the genuine system are safeguarded. One of the benefits of this approach is that new malware is generated through image conversion and an adversarial generative neural network, which has the benefit of predicting and preventing the generation of malware in the future.

Regarding the detection of anomalies in data streams, Demertzis et al. establish a cross-modal dynamic attention neural architecture (CM-DANA), which represents a dynamic attention mechanism that can be trained through harnessing multimodal learning tasks. The data are derived from different cyber modalities and have the benefit of being able to detect suspicious abnormal behaviour.

Mejjaouli and Guizani propose a model based on the fuzzy unordered rule induction algorithm (FURIA), which detects malware associated with portable document format (PDF) malware. A comparative analysis is made of various machine learning models using standard assessment measures. The FURIA-based model was found to outperform other machine learning models.

Considering the problems created by malware and the need to adequately classify viruses, Wu et al. offer guidance on detection rates, for example, and clarify how a static classification model encompassing a malicious code fused with TCN and BiGRU can both extract and integrate the opcode features and the byte features of a malicious code.

Early threat detection has occupied the minds of researchers for some time and López-Vizcaíno et al. focus attention on the time-aware F-score (TaF) metric for early detection, as it considers the number of items/individual elements processed in relation to establishing if an element is an anomaly to be detected or not relevant for detection. The results are validated via an operative system (OS) scan attack. It was concluded that the TaF metric is adequate in terms of a time-sensitive detection system.

Zhang et al. pay attention to detecting phishing scams on Ethereum, and the bagging multiedge graph convolutional network (BM-GCN) scheme is proposed. The BM-GCN (0.877 AUC) scheme was found to outperform other baseline classification methods.

Regarding the unbalanced intrusion detection data vis-à-vis a multi-class classification problem, Bacevicius and Paulauskaite-Taraseviciene evaluate the performance of multi-class classification for network intrusions and utilize the CIC-IDS2017 and CSE-CIC-IDS2018 datasets. The classification performance of six machine learning models was compared, and it was discovered that decision trees using the CART algorithm outperformed the other machine learning models by achieving an average macro $F1$-score of 0.96878.

Supervision control and data acquisition (SCADA) systems are open to attack and can be subject to much disruption. In this context, Söğüt and Erdem carried out research involving five attack scenarios vis-à-vis DDos attacks. By monitoring the SCADA system networks, various models were applied to the obtained data, and it was discovered that the hybrid model and the decision tree were the most suitable and could be used in harmony on real field systems.

Huang et al. focus on cyber mimic defence, and with the need to partition complex networks, multidimensional evaluation metrics were established to assess the effectiveness of cyber mimic defence technology.

Regarding the use of a cyber range to effectively integrate a number of factors in relation to a battlefield environment, Park et al. explain how a multi-cyber range can benefit those engaged in a training environment. There are several advantages: the impacts associated with DDos attacks are highlighted and the interoperability between systems is maintained.

In relation to the security of database management systems (DBMSs) and grey-box fuzzing activity, Wen et al. implement Squill, a grey-box fuzzer, in order to address the challenges associated with DBMS fuzzing. In their study, 30 bugs were found in MySQL, 27 were found in MariaDB and 6 were unearthed in OceanBase, with 9 CVEs assigned. As a consequence, it was proven that Squill was able to locate more bugs in DBMSs as opposed to other known tools.

Additional insights into grey-box fuzzing were provided by Xie et al. Their aim was to rectify the inefficiencies associated with traditional seed scheduling strategies by advocating a seed scheduling strategy guided by untouched edges. As such, a new instrumentation method was put forward. The prototype UntouchFuzz was used to evaluate the experiments against seed scheduling strategies, and 13 vulnerabilities were discovered in the open-source projects and 7 of these had assigned CVEs.

Ransomware attacks are common, and Al-Awadi et al. pay specific attention to evaluating the effectiveness of Windows 11 Pro in relation to its capability to counteract ransomware attacks. A dual examination revealed that Windows 11 Pro does have formidable defences. Recommendations that will benefit technology developers and end-users are provided, which makes an important contribution to cybersecurity knowledge enhancement.

Pan et al. outline a scheme for encrypting linear controllers, the objective of which is to remove security risks and improve security in relation to networked control systems.

The authors use precomputation vis-à-vis data encryption and demonstrate how security can be improved.

With reference to essential cybersecurity control (ECC), Alfaadhel et al. advocate for a comprehensive and customized risk-based cybersecurity compliance assessment system. RC2AS helps staff identify current weaknesses and formalize planning. In addition, the assessment results appear in dashboards. RC2AS can be used to calculate the overall compliance score, which can be considered highly beneficial.

3. Conclusions

As can be deduced from the above, the scope and depth of the knowledge encompassed by the papers that make up this Special Issue will do much to underpin the advancement of cybersecurity, further focusing the minds of senior managers, policy makers and researchers on cyber threat detection and prevention. Indeed, those involved in cybersecurity research are very much involved in defencive actions, and it is hoped that the work of the experts outlined herewith will do much to inspire people to learn more about cybersecurity and engage in cybersecurity research. Guidance is provided in terms of what needs to be achieved to counteract the various types of cyberattack that have proliferated in recent years, and this can be considered beneficial in terms of the issues and challenges that have emerged and are continuing to emerge. The research findings encourage the cooperative spirit of the researchers, and we thank them for sharing their knowledge with us and providing insights that can be drawn upon by a wide audience. It is pleasing to note that those involved in cyber security research are working hard to expand the theoretical base of cybersecurity, which is evolving as an established and distinct body of knowledge.

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

List of Contributions:

1. Ayedh M.A.T.; Wahab, A.W.A.; Idris, M.Y.I. Systematic literature review on security access control policies and techniques based on privacy requirements in a BYOD environment: State of the art and future directions. *Appl. Sci.* **2023**, *13*, 8048. https://doi.org/10.3390/app13148048.
2. Cha, H.-J.; Yang, H.-K.; Song, Y.-J.; Kang, A.R. Intelligent anomaly detection system through malware image augmentation in IIoT environment based on digital twin. *Appl. Sci.* **2023**, *13*, 10196. https://doi.org/10.3390/app131810196.
3. Demertzis, K.; Rantos, K.; Magafas, L.; Iliadis, L. A cross-modal dynamic attention neural architecture to detect anomalies in data streams from smart communication environments. *Appl. Sci.* **2023**, *13*, 9648. https://doi.org/10.3390/app13179648.
4. Mejjaouli, S.; Guizani, S. PDF malware detection based on fuzzy unordered rule induction algorithm (FURIA). *Appl. Sci.* **2023**, *13*, 3980. https://doi.org/10.3390/app13063980.
5. Wu, X.; Song, Y.; Hou, X.; Ma, Z.; Chen, C. Deep learning model with sequential features for malware classification. *Appl. Sci.* **2022**, *12*, 9994. https://doi.org/10.3390/app12199994.
6. López-Vizcaíno, M.; Nóvoa, F.J.; Fernández, D.; Cacheda, F. Time aware F-score for cybersecurity early detection evaluation. *Appl. Sci.* **2024**, *14*, 574. https://doi.org/10.3390/app14020574.
7. Zhang, Z.; He, T.; Chen, K.; Zhang, B.; Wang, Q.; Yuan, L. Phishing node detection in ethereum transaction network using graph convolutional networks. *Appl. Sci.* **2023**, *13*, 6430. https://doi.org/10.3390/app13116430.
8. Bacevicius, M.; Paulauskaite-Taraseviciene, A. Machine learning algorithms for raw and unbalanced intrusion detection data in a multi-class classification problem. *Appl. Sci.* **2023**, *13*, 7328. https://doi.org/10.3390/app13127328.
9. Söğüt, E.; Erdem, O.A. A multi-model proposal for classification and detection of DDoS attacks on SCADA systems. *Appl. Sci.* **2023**, *13*, 5993. https://doi.org/10.3390/app13105993.
10. Huang, Z.; Yuan, Y.; Fu, J.; He, J.; Zhu, H.; Cheng, G. Location-aware measurement for cyber mimic defense: You cannot improve what you cannot measure. *Appl. Sci.* **2023**, *13*, 9213. https://doi.org/10.3390/app13169213.
11. Park, M.; Lee, H.; Kim, Y.; Kim, K.; Shin, D. Design and implementation of multi-cyber range for cyber training and testing. *Appl. Sci.* **2022**, *12*, 12546. https://doi.org/10.3390/app122412546.
12. Wen, S.; Jia, P.; Yang, P.; Hu, C. Squill: Testing DBMS with correctness feedback and accurate instantiation. *Appl. Sci.* **2023**, *13*, 2519. https://doi.org/10.3390/app13042519.

13. Xie, C.; Jia, P.; Yang, P.; Hu, C.; Kuang, H.; Ye, G.; Hong, X. Not all seeds are important: Fuzzing guided by untouched edges. *Appl. Sci.* **2023**, *13*, 13172. https://doi.org/10.3390/app132413172.
14. Al-Awadi, Y.M.; Baydoun, A.; Ur Rehman, H. Can Windows 11 stop well-known ransomware variants? An examination of its built-in security features. *Appl. Sci.* **2024**, *14*, 3520. https://doi.org/10.3390/app14083520.
15. Pan, J.; Sui, T.; Liu, W.; Wang, J.; Kong, L.; Zhao, Y.; Wei, Z. Secure control of linear controllers using fully homomorphic encryption. *Appl. Sci.* **2023**, *13*, 13071. https://doi.org/10.3390/app132413071.
16. Alfaadhel, A.; Almomani, I.; Ahmed, M. Risk-based cybersecurity compliance assessment system (RC2AS). *Appl. Sci.* **2023**, *13*, 6145. https://doi.org/10.3390/app13106145.

References

1. Li, Y.; Liu, Q. A comprehensive review study of cyber-attacks and cyber security: Emerging trends and recent development. *Energy Rep.* **2021**, *7*, 8176–8186. [CrossRef]
2. Lee, J.; Warkentin, M.; Crossler, R.E.; Otondo, R.F. Implications of monitoring mechanisms on Bring Your Own Devise adoption. *J. Comput. Inf. Syst.* **2017**, *57*, 309–318. [CrossRef]
3. Xu, S.; Qian, Y.; Hu, R.Q. Data-driven edge intelligence for robust network anomaly detection. *IEEE Trans. Netw. Sci. Eng.* **2019**, *7*, 1481–1492. [CrossRef]
4. Ma, C. Smart city and cyber-security; technologies used, leading challenges and future recommendations. *Energy Rep.* **2021**, *7*, 7999–8012. [CrossRef]
5. Ullah, F.; Naeem, H.; Jabbar, S.; Khalid, S.; Latif, M.A.; Al-Turjman, F.; Mostarda, L. Cyber security threats detection in Internet of Things using deep learning approach. *IEEE Access* **2019**, *7*, 124379–124389. [CrossRef]
6. Park, M.; Lee, H.; Kim, Y.; Kim, K.; Shin, D. Design and implementation of multi-cyber range for cyber training and testing. *Appl. Sci.* **2022**, *12*, 12546. [CrossRef]
7. Donalds, C.; Osei-Bryson, K.-M. Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents. *Int. J. Inf. Manag.* **2020**, *51*, 102056. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.