10-1-2022

Combining security and reliability of critical infrastructures: The concept of securability

Leandros Maglaras

Helge Janicke
Edith Cowan University, h.janicke@ecu.edu.au

Mohamed Amine Ferrag

10.3390/app122010387
Maglaras, L., Janicke, H., & Ferrag, M. A. (2022). Combining security and reliability of critical infrastructures: The concept of securability. Applied Sciences, 12(20), Article 10387. https://doi.org/10.3390/app122010387

applied sciences

MDPI

Editorial

Combining Security and Reliability of Critical Infrastructures: The Concept of Securability

Leandros Maglaras [1,*], Helge Janicke [2] and Mohamed Amine Ferrag [3]

[1] School of Computer Science and Informatics, De Montfort University, Leicester LE1 9BH, UK
[2] Cyber Security Cooperative Research Centre, Edith Cowan University, Perth 6027, Australia
[3] Department of Computer Science, Guelma University, Guelma 24000, Algeria
* Correspondence: leandros.maglaras@dmu.ac.uk

The digital revolution has made people more dependent on ICT technology to perform everyday tasks, whether at home or at work. The systems that support critical aspects of this smart way of living are characterized as critical, and the security level of such systems is higher as compared to others. The definition of the criticality of a system is a rather difficult exercise, and for that reason, we have seen novel cybersecurity regulations to introduce the idea of digital managed services [1], which include security monitoring, managed network services, or the outsourcing of business processes that are are critical to the functioning, reliability, and availability of Critical National Infrastructures (CNIs). Moreover, ENISA recently issued a new report that deals with supply chain attacks [2]. Those attacks target any chain of the ecosystem of processes, people, organizations, and distributors involved in the creation and delivery of a final solution or product that can be used or incorporated into a CNI, thus further extending the scope of the security posture of a system.

The cybersecurity posture of system or infrastructure can be measured using several methods, including risk management, maturity assessment [3], or posture assessment. Using well-established cybersecurity frameworks such as NIST or ISO, an organization can establish an effective information management system, systematize cybersecurity controls, and improve the security of an organization. These frameworks can be very efficient in helping organizations understand the risks they face, analyze their vulnerabilities and organize their security countermeasures and mitigation plans [4]. The adaptation of those models to specific areas such as banking, healthcare, maritime, or critical components such as industrial systems is still needed [5] in order to achieve better mapping of the system processes and functions.

Reliability, on the other hand, is a measure to estimate the success of a system to perform according to its specifications in terms of time and operation conditions. The reliability is defined as the probability that the system will perform in an adequate manner for a predefined time period. The adequate operation of the system depends on the requirements of the application that are offered by the system. In order to define the reliability of the system, we need to have a very good understanding of the components that comprise the system and the way that these components operate. In order to define the reliability of a system, we need to calculate the reliability of each subsystem or entity and their interconnections and inter-dependencies. The reliability of the system is combined with several metrics such as the Mean Time to Failure (MTTF) and the Mean Time to Repair (MTTR), among others. Reliability analysis and optimization have been used for many years for the development of highly critical systems. In general, reliability evaluation methods can be categorized into two main groups: analytical and simulation-based techniques [6].

The effectiveness of reliability theory in mapping the operation of complex systems, and thus developing highly stable ones, can be used as a basis for the introduction of the securability of systems. Securability can be a metric to represent the ability of the system to operate in a secure manner according to the requirements of the offered services by

Citation: Maglaras, L.; Janicke, H.; Ferrag, M.A. Combining Security and Reliability of Critical Infrastructures: The Concept of Securability. *Appl. Sci.* **2022**, *12*, 10387. https://doi.org/10.3390/app122010387

Received: 8 October 2022
Accepted: 13 October 2022
Published: 15 October 2022

incorporating the basic concepts of reliability. Since errors and failures are factors that affect the correct operation of system, those can and should be part of the securability analysis. The idea of securability lies in the triptych analysis, prediction, and optimization. Concepts such as Mean Time to Attack (MTTA) and Mean Time to Recovery (MTTR) (which are based on the existing incident response and mitigation plans) could be used in order to represent the operation of the system being analyzed. Some first attempts towards this direction have already been made through the use of patterns that combine security and reliability [7] and attack prediction using Markov models [8]. What is missing and is expected to be introduced in the following years is new methodologies that could define the system requirements by incorporating security (and privacy) with reliability (and safety), introducing a new research area under the broad term of securability.

This editorial presents the manuscripts accepted, after a careful peer-review process, for publication in the topic "Cyber Security and Critical Infrastructures" of the MDPI journals *Applied Sciences*, *Electronics*, *Future Internet*, *Sensors*, and *Smart Cities*. The second volume includes sixteen articles: one editorial article and fifteen original research papers describing current challenges, innovative solutions, and real-world experiences involving cybersecurity issues in critical infrastructures.

One major aspect of a smart city involves traffic management using ICT technologies. These technologies come with new vulnerabilities that could expose sensitive data of citizens to hackers. The authors in [9] propose a selective encryption scheme using singular-value decomposition and chaotic systems in order to overcome such issues. The proposed method ensures the confidentiality of video streams originating from devices that have minimal resources and that are mostly used in a smart-traffic management systems. The NIS directive (which is now substituted by the NIS2 Directive) has identified several critical sectors, including transport, and the proposed method could be used as an efficient tool to secure the information that is created and transmitted through a smart traffic system.

When dealing with attacks in critical infrastructures that are usually large complex systems interconnected with several others, the correct prioritization of vulnerabilities is rather a difficult exercise to take. The lack of a proper vulnerability assessment leaves the infrastructure exposed to several attacks that could have devastating physical outcomes when it supports critical services to citizens. The authors in [10] present a vulnerability prioritization model that can reveal characteristics of information-security-related vulnerabilities. Coping with node–edge risk calculation, the authors in [11] propose a vulnerability Correlation and Attack Graph-based node–edge Scoring System. These works reveal the continuous and crucial need for novel vulnerability analysis methods that are based on prioritization and risk analysis.

Dealing with the security and privacy of information during transmission into a digital environment, the authors in [12] propose a GCN algorithm for detecting malicious digital certificates. Malicious certificates can be used in order to hide malicious activities from threat actors. In order to achieve an efficient detection of malicious certificates, the authors design a rules-based method for extracting certificate attributes from documents that are used as features for the classification algorithm. The proposed method is very promising and can be applied in several aspects of electronic transactions where digital certificates are used to link ownership of public keys with the entities that own them. In order to secure transmission of information against tampering and cracking, authors in [13] propose a novel secure communication method based on the message hash chain. The tampering of information has been proven to be very dangerous, especially for industrial control systems that support or offer critical services to citizens, such as energy plants, and solutions that can secure those systems are in need.

On June 2022, the EU Member States agreed on revising the EU Network and Information Security Directive: NIS2. One of the additions of NIS2 as compared to the NIS was the extension of the scope of the NIS with the addition of new sectors, such as the food sector. The authors in [14] discuss the new threats and security challenges that the digitization of agriculture has to face. Among the many open issues, challenges, and future directions that

both organizations and governments will face, the authors propose the development of proper incident response and business continuity plans.

Focusing on the security of industrial control systems (ICS), the authors in [15] propose a configurable dependency model that can be used for risk assessment. The authors identified correctly the specific requirements of an ICS risk model that includes the need to cope with the diversity of experts that cooperate in an ICS along with the need to create a model that can offer an overview of the system at a high level of abstraction while capturing all inter-dependencies. Using the proposed configurable model organisations can save time and resources dedicated to risk assessment and thus be better prepared for cybersecurity incidents.

It has been proven that machine learning principles can be used in order to deploy efficient intrusion detection systems. One-class models have long been proven to be very efficient in circumstances where there is a need for the detection of both known and unknown (novel) attacks; the model must be robust to noise samples and where there is a lack of datasets that include attacks when training the model, all of the above being the standard situation for an ICS. The authors in [16] propose a new IDS that integrates long short-term memory principles into the one-class model and has been tested through extensive experiments on three complex network security data sets.

Following a similar approach, the authors in [17] propose an intelligence system based on machine learning and deep learning approaches to detect serious attacks on ICSs. In another article in this collection, the authors in [18] analyzed the classification of 0-days threats and anomalous intrusion in a novel dataset that includes cloud services. In addition, the authors in [19] propose a malicious anonymous proxy traffic that is based on the principles of deep learning and image transformation. In order to keep the computational overhead of image transformation low, the method converts the sequences of the size and inter-arrival time of the first N packets of a flow into images before applying classification. The proposed methods achieve high accuracy while keeping the sizes of the produced images more than 90% smaller than that of existing image-based deep learning methods All of the aforementioned works of the SI collection are very important since they provide valuable conclusions about the performance of several machine-learning-based intrusion-detection systems against sophisticated attacks, methods to improve their performance and possible future improvements or research directions.

Mobile phones have been used recently for tasks that are not directly linked to communication between users. E-banking, e-commerce, emails, and remote desktop services can help users stay always connected and to perform many of their activities through their mobile devices. The vulnerabilities in these services must be discovered through the execution of the code into a safe or isolated environment. Often, this leads the normal operation of the OS to halt, thus making it unable to offer any services. The authors in [20] try to solve this problem by proposing a secure service provisioning platform that guarantees the execution time of the normal OS while providing hypervisor-level security services. Coping with the same problem from a different perspective, the authors in [21] propose a lightweight, multi-source, fast Android malware detection model by using data from the internal files of the applications in order to build the machine learning models.

The authors in [22] focus on providing a solution for secure health monitoring and for digital twins in adversarial radio environments. The authors propose graph layer security (GLS) in order to secure the information that is transmitted wirelessly by exploiting some of the networked domain's physical dynamics. The method can be robust against both passive eavesdropping attacks and active attacks.

In the last article of this collection, the authors in [23] introduce a testbed for the study of cyber-attacks against a realistic simulation of a nuclear power plant. The testbed integrates a simulated Modbus/TCP network environment containing basic industrial control elements implemented with open-source software components and is validated against several cyberattacks.

Funding: This research received no external funding.

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

References

1. DCMS. Proposal for Legislation to Improve the UK's Cyber Resilience. 2022. Available online: https://www.gov.uk/government/consultations/proposal-for-legislation-to-improve-the-uks-cyber-resilience/proposal-for-legislation-to-improve-the-uks-cyber-resilience (accessed on 1 October 2022).
2. ENISA. Threat Landscape for Supply Chain Attacks. 2021. Available online: https://www.enisa.europa.eu/publications/threat-landscape-for-supplychain-attacks (accessed on 1 October 2022).
3. Aliyu, A.; Maglaras, L.; He, Y.; Yevseyeva, I.; Boiten, E.; Cook, A.; Janicke, H. A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom. *Appl. Sci.* **2020**, *10*, 3660. [CrossRef]
4. Maglaras, L.A.; Jiang, J. Ocsvm model combined with k-means recursive clustering for intrusion detection in scada systems. In Proceedings of the 10th International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness, Rhodes, Greece, 18–20 August 2014; IEEE: Piscataway, NJ, USA, 2014; pp. 133–134.
5. Cook, A.; Smith, R.; Maglaras, L.; Janicke, H. Measuring the risk of cyber attack in industrial control systems. In Proceedings of the 4th International Symposium for ICS & SCADA Cyber Security Research 2016 (ICS-CSR), Belfast, UK, 23–25 August 2016.
6. Maglaras, L.A.; Ferrag, M.A.; Janicke, H.; Ayres, N.; Tassiulas, L. Reliability, Security, and Privacy in Power Grids. *Computer* **2022**, *55*, 85–88. [CrossRef]
7. Buckley, I.A.; Fernandez, E.B.; Larrondo-Petrie, M.M. Patterns combining reliability and security. In Proceedings of the International Conferences on Pervasive Patterns and Applications, IARIA Conferences, Rome, Italy, 25–30 September 2011; pp. 144–150.
8. Holgado, P.; Villagrá, V.A.; Vazquez, L. Real-time multistep attack prediction based on hidden markov models. *IEEE Trans. Dependable Secur. Comput.* **2017**, *17*, 134–147. [CrossRef]
9. Benrhouma, O.; Alkhodre, A.B.; AlZahrani, A.; Namoun, A.; Bhat, W.A. Using Singular Value Decomposition and Chaotic Maps for Selective Encryption of Video Feeds in Smart Traffic Management. *Appl. Sci.* **2022**, *12*, 3917. [CrossRef]
10. Reyes, J.; Fuertes, W.; Arévalo, P.; Macas, M. An Environment-Specific Prioritization Model for Information-Security Vulnerabilities Based on Risk Factor Analysis. *Electronics* **2022**, *11*, 1334. [CrossRef]
11. Shin, G.Y.; Hong, S.S.; Lee, J.S.; Han, I.S.; Kim, H.K.; Oh, H.R. Network Security Node-Edge Scoring System Using Attack Graph Based on Vulnerability Correlation. *Appl. Sci.* **2022**, *12*, 6852. [CrossRef]
12. Liu, J.; Luktarhan, N.; Chang, Y.; Yu, W. Malcertificate: Research and Implementation of a Malicious Certificate Detection Algorithm Based on GCN. *Appl. Sci.* **2022**, *12*, 4440. [CrossRef]
13. Han, M.; Jiang, W. A Secure Communication Method Based on Message Hash Chain. *Appl. Sci.* **2022**, *12*, 4505. [CrossRef]
14. Alahmadi, A.N.; Rehman, S.U.; Alhazmi, H.S.; Glynn, D.G.; Shoaib, H.; Solé, P. Cyber-Security Threats and Side-Channel Attacks for Digital Agriculture. *Sensors* **2022**, *22*, 3520. [CrossRef] [PubMed]
15. Cherdantseva, Y.; Burnap, P.; Nadjm-Tehrani, S.; Jones, K. A configurable dependency model of a SCADA system for goal-oriented risk assessment. *Appl. Sci.* **2022**, *12*, 4880. [CrossRef]
16. Li, Y.; Xu, Y.; Cao, Y.; Hou, J.; Wang, C.; Guo, W.; Li, X.; Xin, Y.; Liu, Z.; Cui, L. One-Class LSTM Network for Anomalous Network Traffic Detection. *Appl. Sci.* **2022**, *12*, 5051. [CrossRef]
17. Alkahtani, H.; Aldhyani, T.H. Developing Cybersecurity Systems Based on Machine Learning and Deep Learning Algorithms for Protecting Food Security Systems: Industrial Control Systems. *Electronics* **2022**, *11*, 1717. [CrossRef]
18. Nkongolo, M.; Van Deventer, J.P.; Kasongo, S.M.; Zahra, S.R.; Kipongo, J. A Cloud Based Optimization Method for Zero-Day Threats Detection Using Genetic Algorithm and Ensemble Learning. *Electronics* **2022**, *11*, 1749. [CrossRef]
19. He, Y.; Li, W. A Novel Lightweight Anonymous Proxy Traffic Detection Method Based on Spatio-Temporal Features. *Sensors* **2022**, *22*, 4216. [CrossRef]
20. Seo, J.; Lee, S.; Kim, K.I.; Kim, K.H. A Fine-Grained Secure Service Provisioning Platform for Hypervisor Systems. *Electronics* **2022**, *11*, 1606. [CrossRef]
21. Peng, T.; Hu, B.; Liu, J.; Huang, J.; Zhang, Z.; He, R.; Hu, X. A Lightweight Multi-Source Fast Android Malware Detection Model. *Appl. Sci.* **2022**, *12*, 5394. [CrossRef]
22. Wei, Z.; Wang, L.; Sun, S.C.; Li, B.; Guo, W. Graph layer security: Encrypting information via common networked physics. *Sensors* **2022**, *22*, 3951. [CrossRef] [PubMed]
23. de Brito, I.B.; de Sousa, R.T., Jr. Development of an Open-Source Testbed Based on the Modbus Protocol for Cybersecurity Analysis of Nuclear Power Plants. *Appl. Sci.* **2022**, *12*, 7942. [CrossRef]