applied sciences

MDPI

Editorial

Digital Transformation and Cybersecurity of Critical Infrastructures

Leandros Maglaras [1,*], Ioanna Kantzavelou [2] and Mohamed Amine Ferrag [3]

[1] School of Computer Science and Informatics, De Montfort University, Leicester LE1 9BH, UK
[2] Department of Informatics and Computer Engineering, University of West of Attica, 122 43 Athens, Greece; ikantz@uniwa.gr
[3] Department of Computer Science, Guelma University, Guelma 24000, Algeria; ferrag.mohamedamine@univ-guelma.dz
* Correspondence: leandros.maglaras@dmu.ac.uk

Critical infrastructures are vital assets for public safety, economic welfare, and the national security of nations. Vulnerabilities of critical infrastructures have increased with the widespread use of information technologies. As Critical National Infrastructures are becoming more vulnerable to cyberattacks, their protection becomes a significant issue for any organization as well as nation. The risks to continued operations from failing to upgrade ageing infrastructures or not meeting mandated regulatory regimes are considered higher given the demonstrable impact of such circumstances.

Due to the rapid increase in sophisticated cyber threats targeting critical infrastructures with significant destructive effects, cyber security of critical infrastructures has become an agenda item for academics, practitioners, and policy makers. In recent years, cyber attacks, especially those targeting systems that keep or process sensitive information, are becoming more sophisticated. Attacks to such critical systems include penetrations to their network and the installation of malicious tools or programs that can reveal sensitive data or alter the behaviour of specific physical equipment. A holistic view, which covers technical, policy, human, and behavioural aspects, is essential to handle the the cyber security of critical infrastructures effectively.

This editorial presents the manuscripts accepted, after a careful peer-review process, for publication in the Special Issue "Cyber Security of Critical Infrastructures" of the MDPI journal *Applied Sciences*. This Special Issue includes thirteen articles: eleven original research papers describing novel ideas, results, and real-world experiences involving critical infrastructures and two review papers focusing on modern training methods for cybersecurity professionals and privacy preservation methods of cloud-based face recognition methods.

Due to the high volume of cyber attacks that have taken place recently on critical infrastructures, a lot of research regarding cyber-attacks has been conducted. However, there has been a lack of research related to measuring cyber-attacks from the perspective of offensive cybersecurity. Motivated by this, the authors in [1] propose a methodology for quantifying cyber-attacks such that they are measurable rather than abstract. The authors first defined and derived the comprehensive offensive cybersecurity framework and taxonomy; then, they performed a content analysis of public reports of cyber-attacks and identified detailed techniques used in cyber-attacks. They created a systematic scoring model based on the offensive cybersecurity framework and calculated the score results of ten fileless and eight Advanced Persistent Threat (APT) group cyber-attacks. The study presented in this article is the first to be conducted to quantify and score cyber-attacks. The basic finding is that APT cyber-attacks have higher scores than fileless cyber-attacks, due to the APT using various ATT&CK techniques. The main limitation is that the proposed approach cannot analyse real malware, but measuring the score of cyber-attacks is meaningful as an initial research step.

Citation: Maglaras, L.; Kantzavelou, I.; Ferrag, M.A. Digital Transformation and Cybersecurity of Critical Infrastructures . *Appl. Sci.* **2021**, *11*, 8357. https://doi.org/10.3390/app11188357

Received: 31 August 2021
Accepted: 8 September 2021
Published: 9 September 2021

As the human element is generally considered the weakest link in a computer system, professional training is now becoming a necessity, not only for raising the users' awareness, but also for training the technical staff to operate the various protection mechanisms that must be acquired. The authors in [2] try to tackle this issue by combining pedagogical methods that promote skill development and security models that capture the security-related aspects of a process. The proposed methodology tackles the incorporation of educational methods to the overall lifecycle of a complete training programme with the dynamic adaptation of the training process to the trainee's particularities. The trainee starts the learning process by consuming the main teaching material (e.g., lectures, tutorials, videos, etc.) and proceeds to more advance learning procedures, involving hands-on experience on emulated/simulated components. The overall method is integrated in the cyber-ranges platform THREAT-ARREST and the trainee is continuously evaluated.

Focusing on cybersecurity training means and methods, the authors in [3] present an analysis of ten cyber ranges that were recently deployed from universities and organizations. The article presents the current state of the art on testbeds and cyber ranges, analyses the findings of a set of structured interviews with organizations that have a testbed and cyber range, and gives insights of modern cyber ranges. A cyber range system is mainly used for one or more of three main objectives: research, training, and exercises. Based on the analysis of state of the art existing cyber ranges, the authors conclude, among other things, that modern CRs should be enriched with novel features, such as various telecommunication capabilities, emulated Banking systems, hospitals, simulated smart grids, automated vehicles, Virtual Cyber Centres of Operation, and many more, in order to be able to offer realistic and tailored training to cybersecurity professionals.

In order to perform vulnerability testing of web applications, different types of analysis security testing (AST) can be used: static (SAST), dynamic (DAST), or interactive (IAST). Authors in [4] produced an analysis that is the first of its kind—to study the best way to combine the three types of security analysis tools for web applications. They investigate the behaviour of the combination of two static tools, two dynamic tools and two interactive tools using a new methodology. The main finding of this research is that combinations integrated by SAST+DAST+IAST tools as Fortify + Arachni + CCE or Fortify + ZAP + CCE reach very good results for high, medium, and low classifications.

The next article of this Special Issue [5] focuses on Higher Educational Institutes of the UK following a recent JISC report, reaffirming that UHEIs in the UK are not well prepared to defend against, or recover from, cyberattacks. HEIs face a constant challenge of balancing public access in the interest of sharing information, whilst protecting their information assets and could be included in a broader group of critical infrastructures. The work presented in this article proposes a novel Holistic Cybersecurity Maturity Assessment Framework (HCYMAF) for HEIs that can be used in order to conduct a gap analysis against 15 security requirements. Moreover, the proposed framework incorporates several regulations and security best practices into one lightweight online self-assessment guide, producing compliance reports against all regulations that the HEI must be compliant with that can be used in order to design appropriate mitigation plans. The research was based into three pilars: structured interviews with experts in the field, a case study on an HEI, and webinars. The proposed framework could be adjusted in order to be applied to organisations in other sectors, e.g., water or power suppliers.

According to several reports (ENISA, Ventures, etc.), ransomware is one of the Top 10 Cybersecurity Threats in 2021. Ransomware's success is largely owed to the relative simplicity with which an attacker can achieve devastating effects, especially when targeting critical infrastructures. Trying to cope with this issue, the authors in [6] propose a ransomware streaming analytics model by integrating a compact set of 24 static and dynamic traits, a hybrid machine learner, a numeral measurement for ransomware's ancestor family attribution, and a statistic formula for a multi-descent ransomware version via a multi-tiered architecture. In order to showcase the efficiency of the proposed model, the authors conduct extensive experiments on a big dataset consisting of 35,000 ransomware versions

of 14 families, 500 versions of 10 malware, and 500 goodware apps aggregated at a different time from different data archives. The proposed solution enriches the accuracy, reduces the mistakes and misclassifications, and shortens the elapsed time versus escalating, big, lifelike, and imbalanced corpora of data.

Dealing with malware that can launch several types of attacks, including ransomware and SolarWinds attacks, is an open issue. The authors in [7] propose an extensible and openly available malware analysis platform entitled Sisyfos. Sisyfos constitutes a significant step in the development of open, modular, and extensible malware platforms that support operational environments, including critical infrastructures. One important aspect that needs to be further investigated is the robustness and fault tolerance of such platforms, especially in boundary cases where samples may lead to system failures.

The next article [8] of the Special Issue proposes an authentication scheme to be employed in rapidly changing variable message format(VMF)-based environments. It is based on the cryptographic hash chain-based authentication technology that includes a time-based one-time password (T-OTP). The proposed lightweight authentication scheme satisfies the demands for a rapidly changing battlefield network and any additional security requirements based on VMF standards. The proposed model could enhance the integrity of tactical message exchanges and reduce unnecessary network transactions and transmission bits for the authentication flow in VMF-based combat network radio (CNR) networks, while ensuring robustness with limited resources.

In most public key infrastructure (PKI) schemes, the public keys are generated by private keys with Rivest–Shamir–Adleman (RSA) and elliptic curve cryptography (ECC). It is now anticipated that quantum computers (QC) will be able to break both RSA and ECC when the technology to manufacture enough quantum nodes becomes available. Paper [9] describes practical ways to generate keys from physical unclonable functions, for both lattice and code-based cryptography and proposes to generate the public–private key pairs by replacing the random number generators with data streams generated from addressable physical unclonable functions (PUFs) to obtain the seeds needed in the post quantum cryptographic (PQC) algorithms. Dissimilar to the key pairs computed by PQC algorithms, the seeds are relatively short, typically 256-bits long.

Devices from the operational technologies (OT) side of this critical infrastructure, which were physically segregated in the past, are now more and more connected to the internet in a series of highly-distributed hierarchical network systems, forming the next generation electric power system or smart grids (SG). SGs are revolutionizing the energy supply sector and this trend is expected to rise in the near future. Unfortunately, SGs have become the target of several serious cyber attacks recently. The authors in [10] focus on such attack scenarios and propose a formal risk assessment framework that is based on threat modelling and probabilistic model checking. The assessment takes into consideration the technological aspects of the SG architecture.

The Industrial Control System (ICS) is an umbrella term that refers to a group of process automation technologies, such as Supervisory Control and Data Acquisition (SCADA) systems and Distributed Control Systems (DCS), which, unfortunately, have been subject to a growing number of attacks in recent years. As they deliver vital services to critical infrastructure—such as communications, manufacturing, and energy among others—hostile intruders mounting attacks represent a serious threat to the day to day running of nation states. Both articles [11,12] focus on detecting vulnerabilities and attacks in an ICS. The former article [11] proposes a pipeline based on existing deep learning models to automatically classify screenshots of ICSs that could be linked to critical infrastructures in order to support the task of detecting vulnerable systems exposed on the internet in real time. The latter [12] introduces interval-valued complex intuitionistic fuzzy relations (IVCIFRs) for recognizing a cyberattack and nullifying its effects.

Advancements in the robotics field have led to the emergence of a diversity of robot-based applications and favoured the integration of robots in the automation of facial recognition tasks. However, this solution faces several security problems. The authors

in [13] studied several approaches for robot-secure face recognition in the cloud environment. By using a set of different algorithms to encrypt a set of images, they trained and tested the robot with various deep learning algorithms and evaluated the efficiency in terms of safety, time complexity, and recognition accuracy using the ORL database.

Author Contributions: All the guest editors contributed equally to this editorial. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Kim, K.; Alfouzan, F.A.; Kim, H. Cyber-Attack Scoring Model Based on the Offensive Cybersecurity Framework. *Appl. Sci.* **2021**, *11*, 7738. [CrossRef]
2. Hatzivasilis, G.; Ioannidis, S.; Smyrlis, M.; Spanoudakis, G.; Frati, F.; Goeke, L.; Hildebrandt, T.; Tsakirakis, G.; Oikonomou, F.; Leftheriotis, G.; et al. Modern aspects of cyber-security training and continuous adaptation of Programmes to trainees. *Appl. Sci.* **2020**, *10*, 5702. [CrossRef]
3. Chouliaras, N.; Kittes, G.; Kantzavelou, I.; Maglaras, L.; Pantziou, G.; Ferrag, M.A. Cyber ranges and testbeds for education, training, and research. *Appl. Sci.* **2021**, *11*, 1809. [CrossRef]
4. Mateo Tudela, F.; Bermejo Higuera, J.R.; Bermejo Higuera, J.; Sicilia Montalvo, J.A.; Argyros, M.I. On Combining Static, Dynamic and Interactive Analysis Security Testing Tools to Improve OWASP Top Ten Security Vulnerability Detection in Web Applications. *Appl. Sci.* **2020**, *10*, 9119. [CrossRef]
5. 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]
6. Zuhair, H.; Selamat, A.; Krejcar, O. A Multi-Tier Streaming Analytics Model of 0-Day Ransomware Detection Using Machine Learning. *Appl. Sci.* **2020**, *10*, 3210. [CrossRef]
7. Serpanos, D.; Michalopoulos, P.; Xenos, G.; Ieronymakis, V. Sisyfos: A Modular and Extendable Open Malware Analysis Platform. *Appl. Sci.* **2021**, *11*, 2980. [CrossRef]
8. Kim, D.; Seo, S.; Kim, H.; Lim, W.G.; Lee, Y.K. A Study on the Concept of Using Efficient Lightweight Hash Chain to Improve Authentication in VMF Military Standard. *Appl. Sci.* **2020**, *10*, 8999. [CrossRef]
9. Cambou, B.; Gowanlock, M.; Yildiz, B.; Ghanaimiandoab, D.; Lee, K.; Nelson, S.; Philabaum, C.; Stenberg, A.; Wright, J. Post Quantum Cryptographic Keys Generated with Physical Unclonable Functions. *Appl. Sci.* **2021**, *11*, 2801. [CrossRef]
10. Vallant, H.; Stojanović, B.; Božić, J.; Hofer-Schmitz, K. Threat Modelling and Beyond-Novel Approaches to Cyber Secure the Smart Energy System. *Appl. Sci.* **2021**, *11*, 5149. [CrossRef]
11. Blanco-Medina, P.; Fidalgo, E.; Alegre, E.; Vasco-Carofilis, R.A.; Jañez-Martino, F.; Villar, V.F. Detecting Vulnerabilities in Critical Infrastructures by Classifying Exposed Industrial Control Systems Using Deep Learning. *Appl. Sci.* **2021**, *11*, 367. [CrossRef]
12. Nasir, A.; Jan, N.; Gumaei, A.; Khan, S.U.; Albogamy, F.R. Cybersecurity against the Loopholes in Industrial Control Systems Using Interval-Valued Complex Intuitionistic Fuzzy Relations. *Appl. Sci.* **2021**, *11*, 7668. [CrossRef]
13. Karri, C.; Cheikhrouhou, O.; Harbaoui, A.; Zaguia, A.; Hamam, H. Privacy Preserving Face Recognition in Cloud Robotics: A Comparative Study. *Appl. Sci.* **2021**, *11*, 6522. [CrossRef]