Manchester Metropolitan University

e-space

Manchester Metropolitan University's Research Repository

Please cite the Published Version

Hammoudeh, Mohammad, Watters, Paul, Epiphaniou, Gregory, Kayes, A S M and Pinto, Pedro (2021) Editorial: Special issue "Security threats and countermeasures in cyber-physical systems". Journal of Sensor and Actuator Networks, 10 (3). 54 ISSN 2224-2708

DOI: https://doi.org/10.3390/jsan10030054

Publisher: MDPI AG

Version: Published Version

Downloaded from: https://e-space.mmu.ac.uk/634405/

Usage rights: CC BY Creative Commons: Attribution 4.0

Additional Information: This is an open access editorial which appeared in the Special Issue Security Threats and Countermeasures in Cyber-Physical Systems, published in Journal of Sensor and Actuator Networks by MDPI

Enquiries:
If you have questions about this document, contact openresearch@mmu.ac.uk. Please include the URL of the record in e-space. If you believe that your, or a third party's rights have been compromised through this document please see our Take Down policy (available from https://www.mmu.ac.uk/library/using-the-library/policies-and-guidelines)

Journal of
Sensor and Actuator Networks

MDPI

Editorial

Special Issue "Security Threats and Countermeasures in Cyber-Physical Systems"

Mohammad Hammoudeh [1,*,†], Paul Watters [2,†], Gregory Epiphaniou [3,†], A. S. M. Kayes [4,†] and Pedro Pinto [5,6,†]

1 Department of Computing & Mathematics, Manchester Metropolitan University, Manchester M1 5GD, UK
2 Department of Security Studies and Criminology, Macquarie University, Sydney, NSW 2109, Australia; paul.watters@mq.edu.au
3 Warwick Manufacturing Group (WMG), University of Warwick, Coventry CV4 7AL, UK; gregory.epiphaniou@warwick.ac.uk
4 Department of Computer Science and Information Technology, La Trobe University, Plenty Road, Bundoora, VIC 3086, Australia; a.kayes@latrobe.edu.au
5 Instituto Politécnico de Viana do Castelo, 4900-347 Viana do Castelo, Portugal; pedropinto@estg.ipvc.pt
6 INESC TEC, 4200-465 Porto, Portugal
* Correspondence: m.hammoudeh@mmu.ac.uk; Tel.: +44-(0)161-247-2845
† These authors contributed equally to this work.

check for updates

Citation: Hammoudeh, M.; Watters, P.; Epiphaniou, G.; Kayes, A.S.M.; Pinto, P. Special Issue "Security Threats and Countermeasures in Cyber-Physical Systems". *J. Sens. Actuator Netw.* **2021**, *10*, 54. https://doi.org/10.3390/jsan10030054

Received: 23 June 2021
Accepted: 20 July 2021
Published: 10 August 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

Wireless, sensor and actuator technologies are often central to sensing or communication critical systems. The last two decades have witnessed a revolution in the design of sensors and actuators that can gather, analyse and communicate data wirelessly to drive intelligent actions in the physical world. Such Cyber-Physical Systems (CPS) add another integration and coordination dimension between the physical and digital worlds. This digital transformation covers manufacturing, critical care, public health, supply chain, and various smart connected systems. For instance, the smart city concept has gained an advantage from new sensing technologies, Internet of Things (IoT), artificial intelligence, cloud computing, big data, smart controllers and adaptive robotics for increasing productivity, fostering industrial growth and shifting economics.

CPS, though still in its infancy, is a fast-moving field with limitless potential. In order to take advantage of what wireless sensor and actuator networks can offer to CPS, many technical challenges have to be overcome before that potential can be achieved. When security is overlooked, CPS can potentially pose serious risks to all stakeholders. There are a large number of potential vulnerabilities and methodologies that are specific to CPS where classical security measures are ineffective. Security advancements have not kept pace with emerging threats to CPS. Security threats targeting the sensing and prediction capabilities of CPS and corresponding countermeasures are under-investigated areas in the literature. For example, limited attempts have been made to combat malicious data injection attacks in sensors and adversarial machine learning. Failure to consider such threats and adversarial models may lead to exploitable system designs that could have disastrous consequences.

This Special Issue is dedicated to publishing cutting-edge research focused on addressing the various fundamental technical open security challenges related to CPS or IoT. It particularly focuses on the future sensor and actuator technologies in the context of smart cities, intelligent transport and healthcare. It also solicits contributions on secure communication technologies and protocols for artificial intelligence-enabled systems.

Six papers have been selected in this special issue that covers the secure design [1], emerging threats [2], counter measures [3,4], operation [5], and forensic investigation [6] methodologies of CPS and IoT systems.

The first article, entitled "Cyber–Physical Systems Forensics: Today and Tomorrow" submitted by researchers from American and Lebanese universities, defines the field of CPS forensics and its technical, organisational and legal dimensions [6]. Then, it reviews

relevant current research efforts in the field and the types of tools and methods they propose for CPS forensics. In addition, the authors discuss the issues and challenges in the CPS forensics field that need to be addressed by researchers and developers of CPS. The authors demonstrate the strong need to study this topic further to provide effective CPS forensics measures. They argue that suitable procedures, tools, regulations, and policies for CPS forensics are extremely important to maintain CPS's security and safety. The authors explain the limitations of existing approaches and use the literature review outcomes to discuss future research avenues to address current challenges and to create more effective, efficient, and safe forensics tools for CPS. This article presents a comprehensive reference for researchers looking to understand the gaps and challenges in CPS forensics.

The second selected article, entitled "Fault Detection Based on Parity Equations in Multiple Lane Road Car-Following Models Using Bayesian Lane Change Estimation" submitted by researchers from Romania, addresses the safety of IoT-enabled transport systems [5]. This paper presents a fault detection analysis of the extension to a multiple-lane car-following model that uses the Bayesian reasoning concept to estimate lane change behaviour. The authors apply the latter model on real traffic data retrieved from inductive loops placed on a road network. They apply standard car-following models separately for each lane showing the ability to perform a lane change action and incorporate a new vehicle into the current lane. The research results highlight the advantages and the critical points of influence in the use of multiple lane car-following models based on probabilistic estimated lane changes. Additionally, this research applied fault detection based on parity equations for the proposed model. The purpose was to deliver an overview of the faults introduced by the behaviour of vehicles in adjacent lanes on the behaviour of the target vehicle. The proposed model was evaluated using Simulink to prove its expected features and performance.

The work by researchers from UK universities entitled "Blockchain and IoMT against Physical Abuse: Bullying in Schools as a Case Study" [2] studies the security benefits of the increasingly applicable blockchain technology to IoT systems. This study investigates the opportunities provided by the Internet of Medical Things (IoMT) data towards next-generation person safeguarding. A new model is developed based on blockchain technology to enable real-time intervention triggered by IoMT data that can be used to detect stressful events, e.g., when bullying takes place. The model utilises private permissioned blockchain to manage IoMT data to achieve quicker and better decision-making while revolutionising aspects related to compliance, double-entry, confidentiality, and privacy. The feasibility of the model and the interaction between the sensors and the blockchain was simulated. To facilitate a close approximation of an actual IoMT environment, the authors clustered and decomposed existing medical sensors to their attributes, including their function, for a variety of scenarios. Then, they demonstrated the performance and capabilities of the emulator under different loads of sensor-generated data. The authors argue the suitability of this emulator for schools and medical centres to conduct feasibility studies to address sensor data with disruptive data processing and management technologies.

The fourth selected article entitled "Distributed Architecture to Enhance Systems Protection Against Unauthorised Activity via USB Devices" by authors from Portuguese universities investigates cyberattacks exploiting Universal Serial Bus (USB) interfaces which are common to CPS edge/gateway systems [4]. The BadUSB is an attack where a USB device's firmware is spoofed and, once mounted, allows attackers to execute a set of malicious actions in a target system. This paper proposes a distributed architecture that uses software blocking to enhance system protection against BadUSB attacks. This architecture is composed of multiple agents and external databases, and it is designed for personal or corporate computers using Microsoft Windows operating system. When a USB device is connected, the agent inspects the device, provides filtered information about its functionality and presents a threat assessment to the user, based on all previous user choices stored in external databases. By providing valuable information to the user, and also threat assessments from multiple users, the proposed distributed architecture

improves system protection. A prototype of the proposed architecture was developed and tested. The filtered information presented in the user interface of the agent intends to aid users in the choice to either accept or block new devices and, from a set of USB devices tested, the additional delay introduced by the agent seems not to significantly affect the user experience.

CPS and IoT devices often suffer from a large number of vulnerabilities and hold a wide variety of information that could be gathered and processed by stego-insiders."An Approach for Stego-Insider Detection Based on a Hybrid NoSQL Database" [3] submitted by authors from Russia addresses the challenge of insider attacks. This article proposes a solution to identify insider attackers threats and their transmission channels. The article provides a review of the related works in terms of insider models and methods of their identification, including techniques for handling insider attacks in Wireless Sensor Networks (WSN), as well methods of embedding and detection of stego-embeddings. This allows singling out the basic features of stego-insiders, which could be determined by their behaviour in the network. In the interests of storing these attributes of user behaviour, as well as storing such attributes from large-scale WSN, a hybrid NoSQL database is created based on graph and document-oriented approaches. The algorithms for determining each of the features using the NoSQL database are specified. The general scheme of stego-insider detection is also provided. To confirm the efficiency of the approach, an experiment was carried out on a real network. During the experiment, a database of user behaviour was collected. Then, user behaviour features were retrieved from the database using special SQL queries. The analysis of the results of SQL queries is carried out, and their applicability for determining the attribute is justified. Weak points of the approach and ways to improve them are indicated.

The review study "Computer Network Attack (CNA) Tactics and Techniques: A Structure Proposal" by the team of researchers from Spanish university studies destructive and control operations, which are a major threat for CPS [1]. In this article, the authors propose the first global approach for CNA operations that can be used to map real-world activities. This approach is designed to identify and structure the techniques followed to perform each of the tactics linked to CNA operations against CPS. The proposed structure is aligned with MITRE ATT&CK, the main effort and the de facto standard to identify and analyse tactics and techniques from advanced threat actors. This proposed novel structure of tactics and techniques significantly contributes to improving the threat model of CNA actors. Additionally, the proposal significantly reduces the amount of effort needed to identify, analyse, and neutralise advanced threat actors targeting CPS. It follows a logical structure that can be easy to expand and adapt.

Articles selected for this special issue contribute to the literature technical solutions and identify security challenges in CPS security and safety. With the increased adoption of CPS and IoT in mission-critical applications such as national infrastructure, it is critically important to develop solutions to ensure their security, resilience and safety. There is a lack of tools, standards and metrics to capture the interconnections amongst CPS that generate new threat landscapes. There are presently no recommended models or techniques for CPS threat landscape modelling. Given both requirements and threats, actors can cover various interactions between the physical and cyber domains. Based on the essential roles that CPS frequently performs, the holistic threat landscape analysis should encompass risks from the whole range of kinetic, cyber-physical, cyber supply-chain, and insider threats. This special issue successfully captured some of these challenges that makes it exceedingly difficult to determine the influence of physical and control processes. Due to the richness and diversity of existing CPS ecosystems, tracing and examining attacks is difficult since threats and vulnerabilities are more difficult to identify and analyse, necessitating further and much needed research in this space.

Funding: This work received no external funding.

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

References

1. Villalón-Huerta, A.; Ripoll-Ripoll, I.; Marco-Gisbert, H. CNA Tactics and Techniques: A Structure Proposal. *J. Sens. Actuator Netw.* **2021**, *10*, 14. [CrossRef]
2. Ersotelos, N.; Bottarelli, M.; Al-Khateeb, H.; Epiphaniou, G.; Alhaboby, Z.; Pillai, P.; Aggoun, A. Blockchain and IoMT against Physical Abuse: Bullying in Schools as a Case Study. *J. Sens. Actuator Netw.* **2021**, *10*, 1. [CrossRef]
3. Kotenko, I.; Krasov, A.; Ushakov, I.; Izrailov, K. An Approach for Stego-Insider Detection Based on a Hybrid NoSQL Database. *J. Sens. Actuator Netw.* **2021**, *10*, 25. [CrossRef]
4. Oliveira, J.; Pinto, P.; Santos, H. Distributed Architecture to Enhance Systems Protection against Unauthorized Activity via USB Devices. *J. Sens. Actuator Netw.* **2021**, *10*, 19. [CrossRef]
5. Pop, M.D.; Proștean, O.; Proștean, G. Fault Detection Based on Parity Equations in Multiple Lane Road Car-Following Models Using Bayesian Lane Change Estimation. *J. Sens. Actuator Netw.* **2020**, *9*, 52. [CrossRef]
6. Mohamed, N.; Al-Jaroodi, J.; Jawhar, I. Cyber–Physical Systems Forensics: Today and Tomorrow. *J. Sens. Actuator Netw.* **2020**, *9*, 37. [CrossRef]