Journal of
Sensor and Actuator Networks

MDPI

Editorial

Cyber-Physical Systems: Security Threats and Countermeasures

Mohammad Hammoudeh [1,†], Gregory Epiphaniou [2,†] and Pedro Pinto [3,4,*,†]

[1] Information and Computer Science Department, King Fahd University of Petroleum & Minerals, Academic Belt Road, Dhahran 31261, Saudi Arabia
[2] WMG, University of Warwick, 6 Lord Bhattacharyya Way, Coventry CV4 7AL, UK
[3] Instituto Politécnico de Viana do Castelo, 4900-347 Viana do Castelo, Portugal
[4] INESC TEC, 4200-465 Porto, Portugal
* Correspondence: pedropinto@estg.ipvc.pt
† These authors contributed equally to this work.

The recent proliferation of sensors and actuators, which is related to the Internet of Things (IoT), provide smart living to the general public in many data-critical areas, from homes and healthcare to power grids and transport. These sensors are gradually moving from only being able to sense their surrounding environment to data processing and decision-making capabilities, with significant implications for explicit e-trust and privacy. As pervasive sensing rapidly expands into new applications, security is failing to keep up with this evolution. The sheer volume of personal and corporate sensor data make it a more attractive target for cybercriminals and state-sponsored espionage, leading an exponential increase in both attack surfaces and threat actors.

The adversarial misuse and security threats in sensor-enabled environments, such as smart cities, are increasingly intertwined with national security and preferential privacy. Hence, governments and organizations are investigating how to mitigate such threats whilse seeking to regulate the secure integration of cyber–physical systems and IoT devices. For instance, the government of the United Kingdom announced new measures to boost cybersecurity in internet-connected devices. A policy document was published on the same day to set out the government's strategy to ensure that consumer IoT is secure by design.

This Special Issue is dedicated to research on the latest developments in security threats and countermeasures regarding sensors and actuators. It aims to explore the critical security challenges, including their legal basis, that face consumers and technology vendors. The focus is on investigating cybersecurity threats and the solutions needed to respond to them.

With the wide adoption of IoT as a sensing and actuation technology, several security and privacy concerns are raised. The adoption of IoT security and privacy guidelines, and the availability of appropriate implementation techniques, is key to addressing security and privacy concerns in IoT systems. In [1], the authors suggest that such guidelines and techniques would greatly assist IoT stakeholders such as developers and manufacturers, paving the road for secure IoT systems to be built and thus reinforcing IoT security and privacy by design. This work discusses the primary IoT security goals and characterises IoT stakeholders. In addition, a comprehensive list of IoT security and privacy guidelines for the edge nodes and communication levels of IoT reference architecture are presented. The article identifies IoT stakeholders, such as customers and manufacturers, who will benefit most from these guidelines. A key contribution of this work is its specifying a set of implementation techniques by which such guidelines can be met, and how possible attacks against the previously mentioned levels can be prevented. This article offers both researchers and practitioners a reference for current challenges in IoT security and privacy guidelines and digital rights management in IoT. It also suggests several open issues that require further investigation.

Bluetooth has become the predominant technology for connecting IoT devices. This is mainly due to its ability to provide a low-energy and low-cost solution to short-range

check for updates

Citation: Hammoudeh, M.; Epiphaniou, G.; Pinto, P. Cyber-Physical Systems: Security Threats and Countermeasures. *J. Sens. Actuator Netw.* **2023**, *12*, 18. https://doi.org/10.3390/jsan12010018

Received: 14 February 2023
Accepted: 14 February 2023
Published: 20 February 2023

radio transmissions. However, Bluetooth lacks a centralized security infrastructure. As a result, it has serious security vulnerabilities, and the need for awareness of its security risks is increasing as the technology becomes more widespread. In [2], the authors present an overview of Bluetooth technology in IoT, including its security, vulnerabilities, threats, and risk mitigation solutions, as well as real-life examples of such exploitations. This study highlights the importance of understanding the attack risks and mitigation techniques involved with using Bluetooth technology on our devices. Real-life examples of recent Bluetooth exploits are presented. Several recommended security measures are discussed to secure Bluetooth communication. This work serves as a comprehensive reference for users to understand the risks involved in using Bluetooth on their devices and recommends mitigation techniques that can be used to protect their devices and information from attackers.

Fog computing is increasingly serving as an architecture for sensor and actuator networks to locally perform a significant amount of computation, storage, and communication, both locally and in the cloud. How to secure IoT applications and networks was studied in [3,4].

Recently distributed computing paradigms, such as Fog and multi-access edge computing (MEC), software-defined networking (SDN), network virtualization and blockchain, were integrated into IoT networks, either combined or individually, to overcome the security challenges facing IoT applications. The work presented in [3] presents a framework that employs an edge computing layer of Fog nodes that are controlled and managed by an SDN network to achieve high reliability and availability for latency-sensitive IoT applications. The SDN network is equipped with distributed controllers and distributed resource-constrained OpenFlow switches. Blockchain is used to ensure decentralization in a trustful manner. Additionally, a data-offloading algorithm is developed to allocate various processing and computing tasks to the OpenFlow switches based on their current workload. Finally, a traffic model is proposed to model and analyze the traffic in different parts of the network.

One way to address the problems associated with running resource-intensive cryptographic-based solutions to IoT security is offloading the additional security-related operations to a more resourceful entity, such as a fog-based node [4]. This article proposes a novel fog security service (FSS) to provide end-to-end security at the fog layer for IoT devices using two well-established cryptographic schemes: identity-based encryption, and identity-based signature. The FSS provides security services such as authentication, confidentiality, and non-repudiation.

At the network edges, the tactile Internet is enabled by IoT and actuating robots.

Latency, availability, reliability, and security are the main design challenges in the tactile Internet system and haptic-based bilateral teleoperation systems. In [5], the authors advocate building a virtual model or model mediated for the remote environment at the edge cloud unit near to the end-user to enable the tactile Internet to be used over any distance with the required latency. Using AI, the proposed virtual model can predict the behaviour of the remote environment; therefore, the end-user can interact with the virtual environment with a high system experience. This article contributes a review of the existing works on model-mediated bilateral teleoperated systems and discusses their availability for the tactile Internet system. It also discusses the security issues in the tactile Internet and the effect of model-mediated systems on the required security level.

Actuation in Industrial Control Systems (ICSs) are responsible for the automation of different processes and the overall control of systems that include highly sensitive potential targets. Given the increased complexity and rapid evolvement of ICS threat landscape, the fact that these systems form part of the critical national infrastructure makes them an emerging domain for cyber exploitation. Existing layered defence approaches are increasingly criticised for their inability to adequately protect against resourceful and persistent adversaries [6]. The authors in [6] study orthogonality to leverage defence advantages against adaptive and often asymmetrical attack vectors. The concept of orthogonality is

relatively new, and this study is one of the first to explore its applciation in an ICS environment. This work articulates a framework in which multiple functional and assurance controls are introduced at each layer of ICS architectural design to further enhance security while maintaining the critical real-time transfer of command and control traffic.

A wide range of sophisticated cyberattacks against corporate and individual systems exist. In this context, the open-source host-based (OSSEC) intrusion detection system (IDS) is commonly deployed. The work in [7] addresses two particular limitations found in the latest OSSEC version, which impact the scalability of this solution when using multiple agents: (1) it is highly complex for the manager to perform deep log analysis centrally, since logs are maintained in each agent and there is no tool for their detailed filtering and analysis, and (2) it is not possible to centrally override the OSSEC actions taken by false-positive or false-negative detections, e.g., to block or unblock one or multiple IP addresses in one or multiple agents. To address these limitations, a novel OSSEC extension is proposed for deployment with the basic OSSEC IDS. This extension comprises changes in the manager and agents and, in the manager, it includes an interface that presents detailed information regarding logs of agents for in-depth analysis and enables the manual blocking or unblocking of one or multiple IP addresses in one or multiple agents. As a result, the proposed OSSEC extension increases this IDS scalability by enabling the system administrator to centrally perform deep analysis tasks and override specific actions as a result of false detections.

Author Contributions: Writing—original draft preparation, M.H.; review and editing, G.E. and P.P. All authors have read and agreed to the published version of the manuscript.

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

References

1. Abdul-Ghani, H.A.; Konstantas, D. A Comprehensive Study of Security and Privacy Guidelines, Threats, and Countermeasures: An IoT Perspective. *J. Sens. Actuator Netw.* **2019**, *8*, 22. [CrossRef]
2. Pau, G.; Arena, F. Smart City: The Different Uses of IoT Sensors. *J. Sens. Actuator Netw.* **2022**, *11*, 58. [CrossRef]
3. Muthanna, A.; Ateya, A.A.; Khakimov, A.; Gudkova, I.; Abuarqoub, A.; Samouylov, K.; Koucheryavy, A. Secure and Reliable IoT Networks Using Fog Computing with Software-Defined Networking and Blockchain. *J. Sens. Actuator Netw.* **2019**, *8*, 15. [CrossRef]
4. Abbas, N.; Asim, M.; Tariq, N.; Baker, T.; Abbas, S. A Mechanism for Securing IoT-enabled Applications at the Fog Layer. *J. Sens. Actuator Netw.* **2019**, *8*, 16. [CrossRef]
5. Ateya, A.A.; Muthanna, A.; Vybornova, A.; Gudkova, I.; Gaidamaka, Y.; Abuarqoub, A.; Algarni, A.D.; Koucheryavy, A. Model Mediation to Overcome Light Limitations—Toward a Secure Tactile Internet System. *J. Sens. Actuator Netw.* **2019**, *8*, 6. [CrossRef]
6. Mackintosh, M.; Epiphaniou, G.; Al-Khateeb, H.; Burnham, K.; Pillai, P.; Hammoudeh, M. Preliminaries of Orthogonal Layered Defence Using Functional and Assurance Controls in Industrial Control Systems. *J. Sens. Actuator Netw.* **2019**, *8*, 14. [CrossRef]
7. Teixeira, D.; Assunção, L.; Pereira, T.; Malta, S.; Pinto, P. OSSEC IDS Extension to Improve Log Analysis and Override False Positive or Negative Detections. *J. Sens. Actuator Netw.* **2019**, *8*, 46. [CrossRef]