Preface

A transformative event known as Industry 4.0 is occurring where countless elements comprising industrial systems are being interfaced with internet communication technologies to form the smart factories and manufacturing organizations of the future. Industry 4.0 and its associated technologies, such as cloud-based design and manufacturing systems and the Industrial Internet of Things, are currently being driven by disruptive innovation that promises to bring countless new value creation opportunities across all major market sectors. However, existing internet technologies are plagued by cybersecurity and data privacy issues that will present major challenges and roadblocks for adopters of Industry 4.0 technologies. Industry 4.0 will face traditional cybersecurity issues along with its very own unique security and privacy challenges. If these challenges are not appropriately addressed, the true potential of Industry 4.0 may never be achieved.

The objective of this book is to provide an overview of cybersecurity for the Industry 4.0 landscape with an emphasis on Design and Manufacturing applications. It covers the technological foundations of cybersecurity within this domain and addresses existing threats faced by Industry 4.0 sectors along with existing state-of-the-art solutions. To provide a holistic perspective, the topic is discussed from the perspectives of both practical implementations in industry and cutting-edge academic research. This way, it benefits practicing engineers and decision makers in industry as well as researchers and educators in the design and manufacturing communities.

In Chapter "Industry 4.0: An Overview of Key Benefits, Technologies, and Challenges", Thames and Schaefer provide details of Industry 4.0 technologies and paradigms in order to provide the reader with a good background of Industry 4.0 basics. The purpose of this chapter is to give the reader a better understanding of the cybersecurity aspects of the remaining chapters in the book.

In Chapter "Customized Encryption of CAD Models for Cloud-Enabled Collaborative Product Development", Cai, Wang, Lu, and Li introduce an innovative and customized encryption approach to support secure product development collaboration. Their goal is to maintain the security of the sensitive information in

CAD models while sharing other information of the models in the cloud for effective collaboration.

Wegner, Graham, and Ribble introduce in Chapter "A New Approach To Cyberphysical Security in Industry 4.0", titled a new paradigm using a direct-to-machine communication approach that limits and protects information flows to internal and subcontracted factory floor devices to complement perimeter security. The authors believe this to be an essential first step in creating secure manufacturing for Industry 4.0.

Chapter "SCADA System Forensic Analysis Within IIoT" introduces the reader to Forensic Analysis within the Industrial Internet of Things (IIoT). In this chapter titled "SCADA System Forensic Analysis within IIoT", Eden et al. focus on the need for incident response when incidents occur within Industry 4.0 environments. The chapter focusses on the forensic challenges and analysis within an IIoT and its physical infrastructure.

In Chapter "Big Data Security Intelligence for Healthcare Industry 4.0", Manogaran et al. provide an overview of how the healthcare industry can be viewed as an Industry 4.0 paradigm. The healthcare industry has started using many types of Internet of Things (IoT) and Industrial Internet of Things (IIoT) technologies. The data generated by healthcare 'things' should be managed with security and privacy in mind. The authors introduce their Meta Cloud-Redirection architecture and describe the security and privacy aspects of it.

In Chapter "Decentralized Cyber-Physical Systems: A Paradigm for Cloud-Based Smart Factory of Industry 4.0" Zhang et al. introduce the conceptual model and operation mechanism of decentralized cyber-physical systems (CPS), which enables manufacturers to utilize a cloud-based agent approach to create an intelligent collaborative environment for product creation. Similar to Chapter "Industry 4.0: An Overview of Key Benefits, Technologies, and Challenges", Chapter "Decentralized Cyber-Physical Systems: A Paradigm for Cloud-Based Smart Factory of Industry 4.0" details many key underlying technologies of Industry 4.0.

Chapter "Applying and Assessing Cybersecurity Controls for Direct Digital Manufacturing (DDM) Systems" introduces the reader to direct digital manufacturing and its cybersecurity needs. In this chapter, Glavach, LaSalle-DeSantis, and Zimmerman address cybersecurity threats to the DDM community. They provide a case study detailing a security assessment performed on an additive manufacturing system and present protocols and recommendations for security best practices for DDM systems.

In Chapter "The Resource Usage Viewpoint of Industrial Control System Security: An Inference-Based Intrusion Detection System", Nair et al. introduce cybersecurity mechanisms for Industrial Control Systems. Their premise is that one can infer CPU load by remotely profiling the network traffic emitted by an ICS device and use that inference to detect potentially malicious modifications to the behavior of the ICS device.

In Chapter "Practical Security Aspects of the Internet of Things", Mehnen et al. introduce a set of key security issues related to the implementation of the Internet of

Things (IoT) in an industrial mechanical engineering context. The authors provide a real-world example concerning remote maintenance of CNC machine tools, which illustrates the different threat scenarios related to IoT in practice. The authors detail various aspects of Big Data and Cloud Manufacturing but focus on improving security at the Edge of IoT, which is where data is collected, transmitted and eventually transferred back to the physical actuators. The authors' aim is to introduce a generic overview of real-world IoT security issues as well as giving a deeper technical example-supported insight into practical considerations for designing IoT systems for practical use in business.

Finally, the book concludes with Chapter "Cybersecurity for Industry 4.0 and Advanced Manufacturing Environments with Ensemble Intelligence". In this final chapter, Thames and Schaefer discuss how machine learning approaches using ensemble intelligence can be achieved. Particularly, the authors describe how cyberattack detection and response mechanisms were integrated into a Software-Defined Cloud Manufacturing architecture. The cyberattack detection algorithm described in this chapter is based on ensemble intelligence with neural networks whose outputs are fed into a neuro-evolved neural network oracle. The oracle produces an optimized classification output that is used to provide feedback to active attack response mechanisms within the software-defined cloud manufacturing system. The underlying goal of this chapter is to show how computational intelligence approaches can be used to defend critical Industry 4.0 systems as well as other Internet-driven systems.

This book is one of the first collections of works related to various aspects of Industry 4.0 and its cybersecurity needs. We hope you find it to be informative and useful for your cybersecurity and Industry 4.0 research efforts.

Atlanta, USA
Bath, UK
Winter 2016/2017

Lane Thames, Ph.D.
Prof. Dirk Schaefer

http://www.springer.com/978-3-319-50659-3

Cybersecurity for Industry 4.0
Analysis for Design and Manufacturing
Thames, L.; Schaefer, D. (Eds.)
2017, XIII, 265 p. 112 illus., 99 illus. in color., Hardcover
ISBN: 978-3-319-50659-3