


Chapter 26

Challenges in Securing Industrial Control Systems Using Future Internet Technologies

Mirjana D. Stojanović

 <https://orcid.org/0000-0003-1073-5804>

Faculty of Transport and Traffic Engineering, University of Belgrade, Serbia

Slavica V. Boštjančič Rakas

 <https://orcid.org/0000-0002-0551-3070>

Mihailo Pupin Institute, University of Belgrade, Serbia

ABSTRACT

This chapter explores challenges in securing industrial control systems (ICS) and Supervisory Control And Data Acquisition (SCADA) systems using Future Internet technologies. These technologies include cloud computing, fog computing, Industrial internet of things (IIoT), etc. The need to design specific security solutions for ICS/SCADA networks is explained. A brief overview of cyber vulnerabilities and threats in industrial control networks, cloud, and IoT environments is presented. The security of cloud-based SCADA systems is considered, including benefits and risks of SCADA migration to the cloud, challenges in securing such systems, and migration toward fog computing. Challenges in securing IIoT are addressed, including security risks and operational issues, key principles for securing IIoT, the functional security architecture, and the role of fog computing. Authors point out current standardization activities and trends in the area, and emphasize conclusions and future research directions.

DOI: 10.4018/978-1-6684-3698-1.ch026

INTRODUCTION

Over the past thirty years information and communication technologies (ICT) have been introduced in the Industrial Control Systems (ICSs) and particularly Supervisory Control and Data Acquisition (SCADA) networks. This implied adoption of open communication standards like Ethernet, Transmission Control Protocol/Internet Protocol (TCP/IP) suite and a variety of wireless standards. Consequently, the problem of increased susceptibility to different forms of cyber security threats appeared, which was verified by a number of successful attacks on worldwide ICS/SCADA systems (Stouffer, Pillitteri, Lightman, Abrams, & Hahn, 2015; Ogie, 2017; Schwab & Poujol, 2018). The need for specific security solutions, tailored to the requirements of industrial control networks, has been recognized as a critical issue from the very beginning.

Nowadays, we are facing with proliferation of the Future Internet technologies, including cloud computing, fog computing, Internet of Things (IoT), mobile computing, big data processing and analytics. The IoT concept is rapidly evolving in different directions. Thus, the Industrial Internet of Things (IIoT) encompasses interconnected sensors, actuators, and other devices networked together with computers' industrial applications, and it represents an essential building block of the Industry 4.0 model (H. Xu, Yu, Griffith, & Golmie, 2018). Energy Internet, also known as the Internet of Energy (IoE) represents a wide area network (WAN), which integrates different types of energy resources, storage and loads, and enables peer-to-peer energy delivery on a large scale (Cao et al., 2018; Bostjancic Rakas, 2020). Heterogeneous IoT (HetIoT) extends the IoT concept to support a variety of heterogeneous wireless technologies and many different applications in daily life and industry (Qiu, Chen, Li, Atiquzzaman, & Zhao, 2018).

Although these technologies bring substantial benefits for the industry regarding information and economic efficiency, cyber security remains a crucial risk factor, which is even more distinct than when using traditional Internet technologies.

Apart from industry efforts (Howard, 2015; Nugent, 2017; Byers, 2018; Aleksandrova, 2019), only a few academic research papers systematically surveyed security issues in ICS/SCADA systems using Future Internet environments (Sadeghi, Wachsmann, & Waidner, 2015; Sajid, Abbas, & Saleem, 2016; Stojanovic, Bostjancic Rakas, & Markovic-Petrovic, 2019).

There are many open issues regarding cyber security of industrial control systems in the Future Internet environments, from the system's level (network security architectures, risk management, security policy implementation), through specific solutions (intrusion detection and prevention systems, encryption, authentication mechanisms), development of dedicated test environments, to definition of security policies that are applied during operational lifecycle. The main objective of this chapter is to emphasize challenges in securing ICS/SCADA systems in such new environments, particularly cloud computing, fog computing and/or IIoT.

The rest of the chapter is structured as follows. The background section explains the reasons for designing specific security solutions for ICS/SCADA networks and presents a brief overview of cyber vulnerabilities and threats in industrial control networks, cloud and IoT environments. In the following section, security of cloud-based SCADA systems is considered, including benefits and risks of SCADA migration to the cloud environment, challenges in securing such systems and migration toward fog computing environment. Further, challenges in securing IIoT are analyzed, including a brief comparison of IoT and IIoT requirements, security risks and operational issues, key principles for securing IIoT, the functional IIoT security architecture and the role of fog computing. The next section addresses

24 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/challenges-in-securing-industrial-control-systems-using-future-internet-technologies/288697

Related Content

Secured Sharing of Data in Cloud via Dual Authentication, Dynamic Unidirectional PRE, and CPABE

Neha Agarwal, Ajay Rana, J.P. Pandey and Amit Agarwal (2020). *International Journal of Information Security and Privacy* (pp. 44-66).

www.irma-international.org/article/secured-sharing-of-data-in-cloud-via-dual-authentication-dynamic-unidirectional-pre-and-cpabe/241285

The Ethical Issues Surrounding Sections 175-178 of the UK's Data Protection Bill

Daniel James Mchenry and Nigel Mckelvey (2021). *Research Anthology on Privatizing and Securing Data* (pp. 2158-2166).

www.irma-international.org/chapter/the-ethical-issues-surrounding-sections-175-178-of-the-uks-data-protection-bill/280277

Performance and Scalability Assessment for Non-Certificate-Based Public Key Management in VANETs

Pei-Yuan Shen, Maolin Tang, Vicky Liu and William Caelli (2012). *International Journal of Information Security and Privacy* (pp. 33-56).

www.irma-international.org/article/performance-scalability-assessment-non-certificate/64345

Access Control, Authentication, and Authorization

Joseph Kizza and Florence Migga Kizza (2008). *Securing the Information Infrastructure* (pp. 180-208).

www.irma-international.org/chapter/access-control-authentication-authorization/28504

Intrusion Detection Systems for Mitigating SQL Injection Attacks: Review and State-of-Practice

Rui Filipe Silva, Raul Barbosa and Jorge Bernardino (2020). *International Journal of Information Security and Privacy* (pp. 20-40).

www.irma-international.org/article/intrusion-detection-systems-for-mitigating-sql-injection-attacks/247425