Editorial

Jörn Müller-Quade, Jürgen Beyerer* and Brandon Broadnax

Editorial

https://doi.org/10.1515/auto-2019-0044

The German initiative Industrie 4.0 aims at making productions more efficient and cost-effective.

In order to achieve this goal, new technologies such as cyber-physical systems, cloud computing and big data analytics are exploited. Via the so-called Internet of Things, numerous machines, sensors and people are connected and able to communicate with each other. Futhermore, cyber-physical systems are able to perform their tasks autonomously based on decentralized decisions which they make on their own. This increased interconnection of devices comes with new risks. For instance, hackers may be able to disable factory machines through remote attacks, enabling them to blackmail the company who owns these machines. Implementing the vision of Industry 4.0 is therefore not possible without relying on cyber security measures.

This special issue deals with various security issues arising in the context of Industrie 4.0. It starts with an essay of *Jens Mehrfeld*, who is working for the Federal Agency for Information Security (German: *Bundesamt für Sicherheit in der Informationstechnik*). Mr. Mehrfeld makes a case for why manufacturing companies should invest more money into cyber security measures. He substantiates his argument by discussing several devastating security incidents.

This special issue continues with three survey articles on the subject.

The article of *Jänicke* considers issues that may arise due to having multiple stakeholders in an Industrie 4.0 context. The paper highlights the possibility of conflicting interests, such as having confidentiality vs. being able to monitor traffic (e. g., for efficient anti-virus applications). These interests not only have to be reconciled, but also supported at the technical level by appropriate protocols and architectures. This article considers several possible conflicts as well as mechanisms and policies for the topic of IT security relevant for Industrie 4.0.

Goncharov et al. discuss several "myths" about how cybersecurity is handled in the industry, for example that no internet connection of a machine supposedly automatically implies security against cyber-attacks. The discussed myths are common statements and situations that security professionals encounter regularily. Several real-world examples to recent attacks are provided for each myth, which make the points understandable and show the significance of the discussed myths. Suggestions are presented on how to deal with theses myths in the future to minimize attack potential.

The paper of *Pfrang et al.* discusses different quality aspects of vulnerability scanners. In order to measure their quality, the scanners are used to find vulnerabilities both in willful vulnerable web servers and in industrial automation and control systems. Five different scanners are analyzed, using three willful vulnerable web servers and seven real hardware components.

Several new methods and schemes are also presented in this special issue.

Paul and Niethammer promote the usage of cryptographic agility for industrial automation. In their paper, they emphasize the effect of post-quantum computing on existing and common security mechanisms that makes it necessary to replace the current security functions with post-quantum ones in the future. In order to achieve this, the authors advocate the usage of cryptographic agility which they define by its three requirements: cryptographic application programming interfaces, secure update mechanisms and documentation of cryptographic primitives. The authors show how to meet these requirements in software-based systems.

The paper of *Genge et al.* presents a key generation scheme to enable data authentication applicable for industrial control systems. In comparison to other solutions, the proposed key generation scheme may be implemented without major changes to the architecture or communication stack of the network. Using key pre-distribution, the

Jörn Müller-Quade, Karlsruher Institut für Technologie KIT, Fakultät für Informatik, Institut für Theoretische Informatik, Am Fasanengarten 5, Geb. 50.34, 76131 Karlsruhe, Germany
Corresponding author: Jürgen Beyerer, Fraunhofer-Institut IOSB, Fraunhoferstr. 1, Karlsruhe, Germany; and Karlsruher Institut für Technologie KIT, Fakultät für Informatik, Institut für Anthropomatik und Robotik, Lehrstuhl für Interaktive Echtzeitsysteme, Haid-und-Neu-Str. 7, 76131 Karlsruhe, Germany, e-mail: juergen.beyerer@iosb.fraunhofer.de
Brandon Broadnax, Karlsruher Institut für Technologie KIT, Fakultät für Informatik, Institut für Theoretische Informatik, Am Fasanengarten 5, Geb. 50.34, 76131 Karlsruhe, Germany

authors eliminate the problem of the limited entropy on industrial control systems. The authors evaluate their approach using a real world scenario and conclude that the approach only adds a reduced overhead to industrial control systems.

Finally, the article of *Gamer et al.* explains how to implement authorization and access control in an OPC Unified Architecture (OPC UA)-based implementation of Asset Administration Shells. In order to corroborate the practical viability of their solution, the authors give an exhaustive validation and evaluation of a prototypical implementation.

We hope that this special issue contributes to a better understanding of the challenges underlying Industrie 4.0 and that the presented solutions inspire many future works.

Bionotes

Prof. Jörn Müller-Quade
Karlsruher Institut für Technologie KIT, Fakultät für Informatik, Institut für Theoretische Informatik, Am Fasanengarten 5, Geb. 50.34, 76131 Karlsruhe, Germany

Jörn Müller-Quade has been a full professor of cryptography and IT security at the Institute of Theoretical Informatics (ITI) at Karlsruhe Institute of Technology (KIT) since 2009. Since 2010, he has been a Director at the FZI Research Center for Information Technology and since 2011 Spokesman of the Competence Center of Applied Security Technology (KASTEL). In 2008 and 2014, he won 1st Place at „Deutscher IT-Sicherheitspreis“ (most distinguished German award in the field of IT security). In 2016, he became member of acatech, National Academy of Science and Engineering, and is now Spokesman of acatech‘s „Themennetzwerk Sicherheit“ and Head of team 3 of the platform „Lernende Systeme“. His research interests include secure multi-party computation, quantum cryptography, formal security models and electronic voting schemes.

Jürgen Beyerer
Fraunhofer-Institut IOSB, Fraunhoferstr. 1, Karlsruhe, Germany
Karlsruher Institut für Technologie KIT, Fakultät für Informatik, Institut für Anthropomatik und Robotik, Lehrstuhl für Interaktive Echtzeitsysteme, Haid-und-Neu-Str. 7, 76131 Karlsruhe, Germany
juergen.beyerer@iosb.fraunhofer.de

Jürgen Beyerer has been a full professor for informatics at the Institute for Anthropomatics and Robotics at the Karlsruhe Institute of Technology (KIT) since March 2004 and director of the Fraunhofer Institute of Optronics, System Technologies and Image Exploitation (IOSB) in Ettlingen, Karlsruhe, Ilmenau, Lemgo. Görlitz. He is Spokesman of the Fraunhofer Group for Defense and Security VVS and he is member of acatech, National Academy of Science and Engineering. Furthermore, he is Head of team 7 of the platform „Lernende Systeme“ and Spokesman of the Competence Center Robotic Systems for Decontamination in Hazardous Environments (ROBDEKON). Research interests include automated visual inspection, signal and image processing, pattern recognition, metrology, information theory, machine learning, system theory security, autonomous systems and automation.

Brandon Broadnax
Karlsruher Institut für Technologie KIT, Fakultät für Informatik, Institut für Theoretische Informatik, Am Fasanengarten 5, Geb. 50.34, 76131 Karlsruhe, Germany

Brandon Broadnax studied Mathematics at KIT from 2006 to 2013. Since 2013, he has been a research associate at the chair of Prof. Müller-Quade. In 2014, he won 1st Place at „Deutscher IT-Sicherheitspreis“ (most distinguished German award in the field of IT security). He finished his PhD in January 2019. His research focuses on formal security models for cryptographic protocols.