IoT4CPS – Trustworthy IoT for CPS

FFG - ICT of the Future
Project No. 863129

Deliverable D9.3.1
Annual Report on the Workshop on Industrial Security and IoT (WISI 2019), ARES & CD-MAKE Conference, Canterbury, UK

The IoT4CPS Consortium:
AIT – Austrian Institute of Technology GmbH
AVL – AVL List GmbH
DUK – Donau-Universität Krems
IFAT – Infineon Technologies Austria AG
JKU – JK Universität Linz / Institute for Pervasive Computing
JR – Joanneum Research Forschungsgesellschaft mbH
NOKIA – Nokia Solutions and Networks Österreich GmbH
NXP – NXP Semiconductors Austria GmbH
SBA – SBA Research GmbH
SRFG – Salzburg Research Forschungsgesellschaft
SCCH – Software Competence Center Hagenberg GmbH
SAGÖ – Siemens AG Österreich
TTTech – TTTech Computertechnik AG
IAIK – TU Graz / Institute for Applied Information Processing and Communications
ITI – TU Graz / Institute for Technical Informatics
TUW – TU Wien / Institute of Computer Engineering
XNET – X-Net Services GmbH

© Copyright 2016, the Members of the IoT4CPS Consortium

For more information on this document or the IoT4CPS project, please contact:
Mario Drobics, AIT Austrian Institute of Technology, mario.drobics@ait.ac.at

Document Control

Title:	Annual Report on the Workshop on Industrial Security and IoT (WISI 2019), ARES & CD-MAKE Conference, Canterbury, UK
Type:	Public
Editor(s):	Julia Pammer (SBA)
E-mail:	jpammer@sba-research.org
Author(s):	Julia Pammer (SBA)
Doc ID:	D9.3.1

Legal Notices
The information in this document is subject to change without notice.
The Members of the IoT4CPS Consortium make no warranty of any kind with regard to this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The Members of the IoT4CPS Consortium shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.
The IoT4CPS project is partially funded by the "ICT of the Future" Program of the FFG and the BMVIT.

(This page is left blank intentionally.)

Abstract

This document seeks to provide insights into the first edition of the workshop on industrial security and IoT (WISI) hosted at the 2019 ARES & CD-MAKE conference in Canterbury, UK.

Contents

1 Workshop on Industrial Security and IoT – disseminating results of IoT4CPS

The factory of the future requires an effective interconnection of machinery, robots, lines, products, sensors and operators to each other and to back-end systems. The industrial propagation environment may also be harsh, mostly metalized, and suffering from man-made, impulsive interference. Industrial IoT priorities are security, low latency, reliability and low cost. However, smart factories are also looking for enhanced services for people and machines that create an added value that is beyond the limits of the production environment, such as indoor localization, smart logistic support, remote maintenance and access to machine data and advanced IT infrastructure, smart tracking of connected components and products.

In order to support dissemination activities in the IoT4CPS project, the AIT and SBA Research have organized the first Workshop on Industrial Security and IoT (WISI 2019). The workshop was hosted as part of the 14th edition of the ARES & CD-MAKE conference, which took place in Canterbury, UK. The objective of the workshop is to support knowledge exchange and networking between researchers in the field of Industrial IoT Security, with the specific focus on flagship project IoT4CPS. The participants in the workshop include the authors of the accepted papers which are coming from Austrian research institutions and industrial parntner and Europe, as well as the general ARES audience which joined the workshop.

The first session started with a keynote speech by AIT cyber security expert Christoph Schmittner, who provided an overview on methods for ensuring security during the entire product life cycle. He also provided insights into the current progress in security and safety standardization activities, with the specific regard to two main IoT4CPS application fields: smart mobility and smart production. The keynote session ended with an open discussion among all participants.

The first accepted paper [1] was a contribution by representatives of the German Research Institute for AI. The authors emphasized on evaluating different methods to leverage network features in intrusion detection systems. They also highlighted the techniques of Matrix Profiles, which they use to detect irregularities in signals coming from industrial control systems. For the attacks that do not manifest through changes in physical signals, the authors propose to build a graph for representing the topology of the network. With this graph, one could understand the valid communication paths in the network, and thus detect different kinds of anomalies.

An application-oriented survey paper [2] was submitted researchers fromthe University of Timisoara, Romania. It was very informative to hear about the applicability of different Elliptic-Curve Libraries in automotive applications. The next paper [5] on “Applicability of the IEC 62443 standard in Industry 4.0 / IIoT” triggered a vivid discussion between the authors and the audience. The participants mostly agreed that the challenges in achieving standard compliance are coming from the loose security zone boundaries in industrial IoT systems as well as remote software updates.

Two additional papers [3,4] provided insights into the latest research results of the IoT4CPS project. The first one, entitled “Requirements and Recommendations for IoT/IIoT Models to automate Security Assurance through Threat Modelling, Security Analysis and Penetration Testing”, dealt with evaluating and improving state-of-the-art methods for security analysis. An additional contribution to the workshop was a submission from Salzburg Research, a partner in the IoT4CPS consortium, entitled “Federated Identity Management and Interoperability for Heterogeneous Cloud Platform Ecosystems”

The organizers of the WISI workshop are satisfied to acknowledge that the WISI workshop provided a strong support for disseminating the IoT4CPS preliminary results and we look forward to continuing the research in IoT4CPS project.

WISI 2019

ARES & CD-MAKE Conference

1.2 WISI 2019 Impressions

Christoph Schmittner (AIT) delivering the WISI 2019 Keynote *Security lifecycles for smart mobility and smart production.*

Christoph Schmittner (AIT) delivering the WISI 2019 Keynote *Security lifecycles for smart mobility and smart production.*

Christoph Schmittner (AIT) delivering the WISI 2019 Keynote *Security lifecycles for smart mobility and smart production.*

Using Temporal and Topological Features for Intrusion Detection in Operational Networks
Simon Duque Anton (Deutsches Forschungszentrum für Künstliche Intelligenz GmbH, Germany), Daniel Fraunholz (Deutsches Forschungszentrum für Künstliche Intelligenz GmbH, Germany)

2 ARES & CD-MAKE Conference

This year´s ARES & CD-MAKE conference took place at the University of Kent in Canterbury, UK from August 26-29, 2019. Accommodation on campus provided a great possibility for 230 participants from 33 countries to discuss the various aspects of security from early morning until late evening. For the third year in succession, the International IFIP Cross Domain Conference for Machine Learning & Knowledge Extraction (CD-MAKE) was co-located with ARES 2019.

21 full papers (**acceptance rate: 20.75%)** and 9 short papers were presented in the ARES main track. This year´s schedule offered participants a vast range of topics within 19 workshops (3 of them in the context of the EU Projects Symposium). Several social events provided good networking opportunities as well as insights into Canterbury´s surroundings and culture.

The **International Conference on Availability, Reliability and Security** ("ARES") brings together researchers and practitioners in the area of dependability since 2006. ARES highlights the various aspects of security – with special focus on the crucial linkage between availability, reliability and security.

ARES aims at a full and detailed discussion of the research issues of security as an integrative concept that covers amongst others availability, safety, confidentiality, integrity, maintainability and security in the different fields of applications.

ARES will emphasize the interplay between foundations and practical issues of security in emerging areas such as e-government, m-government, location-based applications, ubiquitous computing, autonomous computing, chances of grid computing etc. ARES is devoted to the critical examination and research challenges of the various aspects of Secure and Dependable Computing and the definition of a future road map.

Selected papers that are accepted and presented at the ARES Conference are being published after further revision, in special issues of international journals (e.g. Springer EURASIP Journal on Information Security). ARES 2019 was published by the International Conference Proceedings Series published by ACM ICPS. ARES is ranked as B-conference in CORE. Qualis (backed by Brazilian Ministry) ranked ARES and Esorics as leading security conference in Europe (A2).

2.2 WISI at ARES & CD- MAKE 2020

The second edition of WISI is scheduled to be hosted at ARES & CD-MAKE 2020 at the University College of Dublin, Ireland. The topics of interest will cover dependability design methods for IoT, automated test case generation, secure connectivity to life cycle data management, usable security and much more. We aim to use WISI 2020 as an opportunity to

disseminate the most mature IoT4CPS project outcomes within the scientific and industrial community.

References

[1] Simon Duque Anton, Daniel Fraunholz and Hans Dieter Schotten: Using Temporal and Topological Features for Intrusion Detection in Operational Networks

[2] Lucian Popa, Bogdan Groza and Pal-Stefan Murvay: Performance Evaluation of Elliptic-Curve Libraries on Automotive-Grade Microcontrollers

[3] Ralph Ankele, Stefan Marksteiner, Kai Nahrgang and Heribert Vallant: Requirements and Recommendations for IoT/IIoT Models to automate Security Assurance through Threat Modelling, Security Analysis and Penetration Testing

[4] Nirojan Selvanathan, Dileepa Jayakody and Violeta Damjanovic-Behrendt: Federated Identity Management and Interoperability for Heterogeneous Cloud Platform Ecosystems

[5] Björn Leander, Aida Causevic and Hans Hansson: Applicability of the IEC 62443 standard in Industry 4.0 / IIoT