IoT4CPS – Trustworthy IoT for CPS

FFG - ICT of the Future
Project No. 863129

Deliverable D9.3.2
Annual Report on the Workshop on Industrial Security and IoT (WISI 2020), Remote ARES & CD-MAKE Conference

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

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 2020), Remote ARES & CD-MAKE Conference
Type:	Public
Editor(s):	Julia Pammer (SBA)
E-mail:	jpammer@sba-research.org
Author(s):	Julia Pammer (SBA)
Doc ID:	D9.3.2

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 2020 Remote ARES & CD-MAKE Conference.

Contents

1 Workshop on Industrial Security and IoT – disseminating results of IoT4CPS 6
2 ARES & CD-MAKE Conference 7
2.2 WISI at ARES & CD- MAKE 2021 8

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 localisation, smart logistic support, remote maintenance and access to machine data and advanced IT infrastructure, smart tracking of connected components and products.
This year we organized a 2nd Workshop on Industrial Security and IoT, co-located with ARES conference. This event focuses on bringing researchers together in order to exchange ideas and present their current work. Unfortunately, due to well-known situation with the coronavirus, the event was held online. Similar to last year, our Program Committee was strongly supported by the IoT4CPS scientific and industrial community. Last but not the least the workshop helped further deepen the collaboration between AIT and SBA research. This year WISI workshop accepted 5 submissions, with the focus on cybersecurity for IoT, mobile devices and industrial devices, as well as network intrusion detection and testing for security.
The first presented paper was from our colleagues from Software Competence center Hagenberg entitled “A Semi-Supervised Approach for Network Intrusion Detection”. This paper is considering a relatively novel approach for building intrusion detection systems for computer networks, based on semi-supervised learning methods, specifically on undercomplete autoencoder.
The discussion continued with a very interesting presentation from TU Graz: AndroPRINT: Analysing the Fingerprintability of the Android API. This paper stood out as the most prominent, due to the impact of topic of the paper. The authors were able to discover several information sources that can be used to fingerprint and track Android devices. The authors thereby only consider information that can be collected by an app without user's explicit consent, thus posing a realistic threat to the privacy of mobile users. The authors present a large number of unique identifiers that can be extracted without the user's knowledge, including list of ringtones or even the user's email address on recent Samsung devices.
The central time slot of the workshop was reserved for researchers from Villach and Eindhoven with their work: RESCURE: A security solution for IoT life cycle which advocated the usage of SRAM PUFs for securing the lifecycle of IoT devices, including secure storage of sensitive data, e2e encryption, and secure software updates.

The fourth presentation on improving security in I4.0 by the authors from National Research Council of Italy. This work presents a framework that provides ongoing control on actions execution in the industrial environment exploiting the OPC Unified Architecture (OPC-UA) framework and the Usage Control (UCON) paradigm. The authors provide a fine-grained usage control model, referred as OPC-UCON, satisfying security and privacy needs of the OPC-UA framework.
The WISI workshop was concluded with the work on security testing entitled Automated Security Test Generation for MQTT Using Attack Patterns. This paper presents a method for automated test generation for security testing, in which the tests are based on attack patterns. The proposed approach makes reuse of previously successful attacks to derive security tests. The authors apply the approach on different implementations of the MQTT broker and demonstrate its effectiveness by detecting a number of errors and failures.

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.

More information

2 ARES & CD-MAKE Conference

This year´s ARES & CD-MAKE conference was conducted as a remote event from August 25-28, 2020 with over 300 participants from 43 nations. For the third year in succession, the International IFIP Cross Domain Conference for Machine Learning & Knowledge Extraction (CD-MAKE) was co-located with ARES 2020.

26 full papers and 7 short papers were presented in the ARES main track. This year´s schedule offered participants a vast range of topics within 16 workshops (3 of them in the context of the EU Projects Symposium).

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 2020 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 2021

The third edition of WISI is scheduled to be hosted at ARES & CD-MAKE 2021 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 2021 as an opportunity to disseminate the most mature IoT4CPS project outcomes within the scientific and industrial community.