Cybersecurity for the Industrial Internet of Things (C4IIoT) Spring School 2022

Virtual 24/05/2022

Registration Link: <Click Here>

Program (all times CET)

10h00-11h00: *Introduction to the C4IIoT project with an architecture overview*
Srdjan Skrbic, University of Novi Sad

11h00-12h00: *Information Security Risk Management and Standardization on IoT Cybersecurity*
Hervé Cholez, Luxembourg Institute of Science and Techonology

12h00-12h15: Short break

12h15-13h15: *Multi-factor Authentication and Key Exchange for IoT*
Bowen Liu, Luxembourg Institute of Science and Techonology

13h15-14h30: Lunch break

14h30-15h30: *Securing the infrastructure, Detecting and Mitigating threats*
Giorgios Stamatis, Information Technology for Market Leadership (ITML)

15h30-16h30: *C4IIoT automated mitigation search: a Constraint Object-Oriented Logic Programming approach*
Camilo Correa, University of Paris 1 Panthéon-Sorbonne

Cybersecurity for the Industrial Internet of Things (C4IIoT) Spring School 2022

Details on the presentations:

Title: *Introduction to the C4IIoT project with an architecture overview*

Abstract: C4IIOT project aims to design, build and demonstrate a novel and unified Cybersecurity 4.0 framework that implements an innovative IoT architecture paradigm to provide an end-to-end holistic and disruptive security-enabling solution for minimizing the attack surfaces in Industrial IoT systems. C4IIOT bridges cyber assurance and protection, machine (deep) learning (ML/DL), edge/cloud computing, blockchain and Big Data technologies to provide a viable scheme for enabling security and accountability, preserving privacy, enabling reliability and assuring trustworthiness within evolving IIoT applications and processes.
In this talk, we give an overview of project objectives, present use cases, and explain details of the final system's architecture.

Title: *Information Security Risk Management and Standardization on IoT Cybersecurity*

Abstract: Nowadays, systems and enterprises are strongly interconnected and need to interact continuously. In this context, the occurrence of an event in one system may lead to a serious risk in another. Thus, information security has become a central concern inside organisations, but it remains quite difficult for most entities to implement and maintain a high level of information security. It is clearly acknowledged that, in complex systems like the Internet of Things (IoT), to consider an infrastructure as fully secure, although desirable, is not realistic. In this context, risk management has become both a key aspect for dealing with security and a main trust vector. This presentation will thus explain how to implement an Information Security Risk Management and take appropriate technical and organizational measures to manage the risks posed to security of IoT. This talk will also cover standardization on cybersecurity and IoT and their challenges.

Cybersecurity for the Industrial Internet of Things (C4IIoT) Spring School 2022

Details on the presentations (continued):

Title: *Multi-factor Authentication and Key Exchange for IoT*

Abstract: During this session, the speaker will introduce the elementary information about the general authenticaton mecanisem and its vulnarability, in addition with the Internet of Things (IoT) respective. Besides, the speaker will describe the fundamental idea of designing an Authenticated Key Exchange (AKE) protocol and the desired security properties. In order to demonstrate how to properly design an AKE protocol, a brief overview of the IoT friendly protocol they proposed at 24th information security conference in 2021 will be presented. And the session will be concluded with the challenges we face today.

Title: *Securing the infrastructure, detecting and mitigating threats*

Abstract: The C4IIoT framework increases the security of the Industrial IoT environment and facilitates with the detection and mitigation of threats endangering the smooth operation of logistics pipelines and the production facilities. Following the data from their creation on the IoT edge to their analysis and presentation to user, the presentation will demonstrate how multiple different technologies work in synergy in order to increase security of the infrastructure and verify the integrity of the data.

Title: *C4IIoT automated mitigation search: a Constraint Object-Oriented Logic Programming approach*

Abstract: Critical infrastructures must be able to mitigate, at runtime, suspected ongoing cyberattacks that have eluded preventive security measures. To tackle this issue, and within the context of the larger C4IIoT framework, we designed and implemented a tool to propose sets of semi-automatically enforceable actions based on a specication of a suspected attack. This tool is based on and benefits from the unique properties of the alignment of several declarative programming paradigms within a single programming environment.