IE 2022 Tutorial Proposal: An Overview of the Security Challenges of IoT Solutions

- **Names and Affiliations of Speakers**

Arthur Desuert, PhD student
Laboratoire de Conception et d'Intégration des Systèmes (LCIS)
Université Grenoble Alpes

Amir Ali Pour, PhD student
Laboratoire de Conception et d'Intégration des Systèmes (LCIS)
Université Grenoble Alpes

- **Abstract, objectives and motivation**

Connected devices are getting really present in the daily life of human users. These devices are the foundation of smart spaces which aim at offering useful services like remote control of users' homes or efficient energy usage across large buildings. However they also raise significant challenges, concerning for instance their security. In this tutorial, we aim at clearly defining some of those security challenges. To do so, we present a classical architecture to connect devices and applications together for commercial or industrial deployment of smart spaces. We then present for several key points of this architecture the associated security needs. To meet those needs, current technologies are presented as well as proof of concept of recent research work in this area. The presentation also features a set of potential points of combinatory utilization of Physically Unclonable Function (PUF); a pervasively expanding hardware primitive, and machine learning methods, that can open in conjunction with each-other some interesting protocols for IoT security. To illustrate the presentation, a demonstration of a real-life IoT scenario illustrating the presented challenges conclude the tutorial. At the end of the tutorial, the attendees will have a clear understanding of the security challenges of IoT solutions and some ways to address them.

- **Keywords**

IoT, architecture, secure storage, secure transmissions

- **Intended Audience**

  The tutorial is intended for researchers and industrial actors working in the field of IoT solutions; covering connected devices, communication protocols and IoT platforms. The tutorial is an introduction to the security challenges of the IoT field. No specific knowledge is required, the basics are covered during the tutorial.

- **Content outline**

  1. Security needs for IoT.
  2. Basic IoT architecture.
  3. Security of communication protocols.
  4. Embedded security for connected devices.
  5. Integration into IoT platforms.
  6. Synthesis and perspectives.

- **Description**

  The Internet of Things market is rapidly growing and with it the development of new applications, connected devices, protocols, etc.. As IoT solutions can process sensitive data and affect the environment, it is vital to integrate appropriate security measures and choices in the design of those solutions. However, to adequately choose those security measures it is necessary to have a good understanding of the IoT field, with its particularities and challenges. This tutorial aims at offering to attendees a background on the IoT field and its specific security challenges, (so they can make wise design choices when developing their next IoT solution). Some promising security solutions will be presented, which can represent opportunities for new research subjects or integration into future products.

- **Teaching mode**

  The tutorial is planned to be face-to-face only, with a live demonstration. The expected duration of the tutorial is one hour and a half. If needed the tutorial can be presented online, using a Zoom session and with the demonstration being a pre-recorded video.

- **Materials**

  The audience will have access to the presentation slides of the tutorial.

- **Additional information**

  N/A

- **Bio-sketches**

  Arthur Desuert is currently a PhD student at the Université Grenoble Alpes. He received in 2020 a Master's degree in Computer Science from the Université Grenoble Alpes, in France. His research is about the secure integration of connected devices in pervasive applications; understanding the implied challenges, the benefits and limitations of current solutions to design new ways of securing IoT.

  Amir Ali Pour is a PhD student at the Université Grenoble Alpes (UGA). He received his Master's degree in Engineering from Grenoble INP in 2019. His PhD thesis work is specialized in designing and evaluating machine learning and deep learning based secured solutions for PUF computing for resource constrained cyber-physical systems.