<u>Title</u>: “Implementation of a Light-Weight Security Framework for IoT”

The emergence of the Internet of Thing (IoT) paradigm pushes our daily life to be as digital as possible. Billions of devices, people and eventually services would be expected to interconnect and exchange data and useful information. While it creates new opportunities, IoT also presents fundamental challenges related to security and privacy. To establish secure connections among people, process, data and things, security needs to be ubiquitous. The physical and cyber security must work collaboratively to protect the networks, applications, devices, data and users which are the building blocks of IoT. Due to the increase in connected devices, big data and automation, system data need to be processed as securely as possible.

In this context, this internship will address the Security Analytics for IoT, which will provide a big picture on the concepts, techniques, applications, and prominent research directions in this area. Indeed, access control policy management is a well-mastered art relying on standardized and reliable architectures. Nonetheless, such architectures are still limited to support scalable contextual permissions in the access control management. Context-sensitive access control enables to take access control decisions based on one or more “Contexts” related to a human being or a physical object (e.g., location, situation, level of trust or reputation of surrounding entities…). Hence, the main objective for this work is to develop a proof-of-concept for a light weight security policy, implementing an access control scheme based on security tokens.

After a state-of-the-art analysis related to security and privacy aspects in the IoT ecosystem, the selected intern would work on the following aspects:

- Analyze the risks and vulnerabilities related to a specific scenario (smart hotel room, smart car door lock, etc.).
- Design a Lightweight context-sensitive access control scheme with specific security policies in order to provide keys and locks for opening/locking the access to resources and assets in the Internet of Things (IoT).
- Implement a showcase scenario using an android phone application to securely access smart IoT device (open smart lock, retrieve sensitive information, etc.…)

<u>Keywords</u>: Internet of Things, Network Security, Privacy Protection, Access control, Public Key Infrastructure (PKI).

Supervisors: Prof. Sidi Mohammed Senouci and Dr. Ayoub MESSOUS, University of Bourgogne, Nevers

Starting date: Early 2019

Duration: 5- months

Place: DRIVE Lab in Nevers, University of Burgundy, France.

Expected profile: The required initial training is BAC+5 (last year internship of Engineering School or Master 2) in Computer science or Telecoms, with Good mathematical background and a strong knowledge in network security, as well as practical skills with programming languages and software tools (e.g., Java, Android, Arduino). Above all, the applicant must be dynamic with communication and teamwork skills, motivated to learn quickly and work effectively on challenging research problems.

Selection process: Potential candidates are requested to send their resume and latest transcripts (eventually recommendation letters) to:

Prof. sidi-mohammed.senouci@u-bourgogne.fr
Dr. ayoub.messous@u-bourgogne.fr