Research project
for students from Master 2 WET

Start of the project: *February 3, 2020*
End of the project: *July 3, 2020*
Oral presentation: *between 1 and 6, July 2020*

Laboratory: **IETR**

Subject (title): **Compatibility between security and reliability mechanisms in IoT systems**

Subject description:
Internet of Things (IoT), originally addressing the public use, gathers a great number of *objects*, sensors and generated data.
However, the objects (connected devices) and data handled, stored and generated by these devices might be critical at different levels: from devices manipulating personal or private data, to devices responsible for the proper functioning of production lines for instance.
It is therefore necessary to take into account the dependability of a system, including among others, reliability (resilience against possible malfunctioning due to natural events), and security properties (resilience against possible malfunctioning due to voluntary attacks). However, despite this global definition of dependability (also called safety), today, we are still not able to realistically evaluate the degree of reliability and security of such electronic systems. State-of-the-art clearly shows that the studies simultaneously addressing both, reliability and security are (very) few. Indeed, numerous work and contributions exist but have only considered one of these two properties. But security and reliability are based on contrasting principles; reliability is generally based on determinism principles, whereas security is often based on the integration of randomness in values and behavior. It is therefore necessary to study and to evaluate the compatibility of state-of-the-art solutions in order to simultaneously answer to the reliability and security requirements.
Finally, this evaluation must encompass both, theoretical study and practical experimentation.

This master project will focus on IoT systems (connected devices and communication network) and will investigate the impact on security of current state-of-the-art solutions initially proposed to answer to reliability requirements, and vice versa (examples are hardware and software duplication/triplication, communication filtering/monitoring, software/hardware isolation of critical applications or tasks, among others). This work will be based on a theoretical study of current state-of-the-art contributions, as well as on the practical evaluation of the degree of reliability and security. According to the progress of this project a final contribution will be to enhance current security/reliability mechanisms in order to answer both domains requirements simultaneously.

This internship work will leverage the knowledge and motivation of the project candidate but also the expertise of the SYSCOM team in IETR lab in reliability and security domains. Finally, for practical experimentations, the candidate will leverage the lab equipment for security analysis/audit (communication buses, memory dump, ...), and logical and physical attacks equipment (side-channel attacks and fault injection on the devices themselves).

This project continues the work of a previous one, therefore the first experimentations results (theoretical reports, practical equipment manuals, raspberry PI network and manual) will be provided as a basis for this project.

Particular required knowledge:

The student is required to be interested in IoT, and/or security, and/or networks. Also the student is required to have good skills in programming (C language/Python).

Starting bibliography (provide 3 papers references):

- Internet of things security: A top-down survey, Ahmad-Reza Sadeghi et al., in ACM/EDAC/IEEE Design Automation Conference (DAC), 2015.
- Internet of things security: A top-down survey, Djamel Eddine Kouicem et al., in Computer Networks, Volume 141, 2018.
- Etude et conception de mécanismes de rupture et de filtrage de protocols industriels, Peter Rouget, PhD Thesis, English version, 2019.

Contact (name, email, #room): Maria Méndez Real, maria.mendez@univ-nantes.fr, IETR, 1st floor, room # C110

Main supervisor: Maria Méndez Real (IETR, France)

Other(s) supervisor(s): Sébastien Pillement (IETR, France)