CERES Research Internship: Digital Twin for Securing Building Management Systems

Institut Polytechnique de Paris

Internship start: February 2022

Keywords — building management system, digital twin, cyber-physical security

Context

Information systems are increasingly complex and spreading in every sector, often built from off-the-shelf components, with little to no security guarantees whatsoever. In order to regain its sovereignty, a State needs to build its cybersecurity posture from certified software and hardware stacks, security-wise. Testing is thus necessary to assess the level of security of a system. It highly depends upon what and how a targeted (sub-)system is tested. Additionally, testing a real system is often too expensive or simply infeasible for safety reasons. To that end, a certain amount of simulation/emulation is often leveraged to compensate. Recently, the concept of digital twin (DT) has been considered to model complex and/or large industrial systems, for which safety requirements prevent any direct testing. DT proposes a replica of a complete system by using data related to the state of the system under test, expert knowledge or even data from similar devices. Its usage seems to have found applications in industrial systems [1, 2] as it represents a good trade-off between cost and realism, but it is still emerging for complex information systems.

Digital twins have been proposed and implemented for a broad range of applications ranging from aerospace, to electricity, to automobile, to healthcare, and now, buildings. As a matter of fact, buildings are getting increasingly equipped with sensors and actuators, enabling cyber-physical command and control of a number of subsystems: power, water, ventilation, lighting, etc. Such control-and-command systems are termed building management systems (BMS). As any cyber-system, the BMS relies on a networking infrastructure and can even be accessed remotely for off-site management. BMS obviously incur cyber-risks, which should be addressed, as any threat not prevented could turn into physical damages to the building or its inhabitants.

This internship aims to survey the state of the art of building management systems to understand what is the actual level of information of the physical assets, as well as the information aspects to evaluate the cyber-risks. A number of subsystems of a BMS will then be modelled so as to take into account security risks. This will enable BMS to anticipate security risks and measure the impact in case their security is compromised. Early prototypes will be integrated in a project platform. The models can also take into account data from other BMS already deployed on campus.

Activities

- survey of building management systems (BMS)

- study of the security of BMS
- modelling of cyber-threats to BMS
- integration to subsystems within a platform
- *(optional) integration of data sources from the campus' BMS*

Practical information

The internship will take place jointly at SAMOVAR and LTCI laboratories, Institut Polytechnique de Paris, in Palaiseau. It will be 5 to 6 months long.

Applicants are about to complete their Master 2 level degree (or equivalent engineering school degree) and should have the following skills:

- strong knowledge in a modern programming language
- skills in system modelling, or at least practice in modelling languages
- knowledge in cybersecurity risk modelling

The internship topic is linked to a Ph.D offer in the context of the CERES project (funded by the French Agency for Defense Innovation (AID)). **Applicants MUST be European nationals and WILL be subjected to a defense authorization process before starting**. Applications (resume, motivation letter, academic transcripts, recommendation letters) must be sent to `gregory.blanc[at]telecom-sudparis.eu`, `jean.leneutre[at]telecom-paris.fr` and `olivier.levillain[at]telecom-sudparis.eu`.

References

[1] A. Bécue et al. A New Concept of Digital Twin Supporting Optimization and Resilience of Factories of the Future. *Applied Sciences*, 10(13):4482, 2020.

[2] M.J. Kaur et al. *Digital Twin Technologies and Smart Cities*, chapter The Convergence of Digital Twin, IoT, and Machine Learning: Transforming Data into Action. 2020.