Development of a cyber-physical simulator of an indoor localization platform for vulnerability analysis and countermeasure evaluation

Position: Internship (Master level)

Laboratory: Univ. Grenoble-Alpes, Grenoble INP * LCIS *(Valence, France)*
**Grenoble Institute of Engineering*

Team: CTSYS ***(****Embedded & Pervasive Systems Security)*

Keywords: *cyber-physical systems, indoor localization, IoT, cybersecurity, system-level countermeasure.*

Indoor localization is a growing field of the IoT, which is found in various applications such as robot navigation, industrial supervision or location-based access control. Despite being widely used in sensitive environment such as factories or hospitals, most off-the-shelf positioning systems remain unsecured, often neglecting basic cryptographic means available. Various communication technologies can be used for localization purposes, and Ultra-Wide Band (UWB) in particular has the best performances, with a potential of 10 cm accuracy and 1000 Hz refresh rate.
As a consequence, we developed an indoor secure UWB localization platform towards positioning and security experiments. This platform is fully open at every protocol layer, allowing experimenting with attacks and evaluating countermeasures. Tags position are computed and displayed in real time by a 3D engine and the whole dataset and positions are logged, such as replaying scenarios with different parameters.
However, some security scenarios need to be evaluated on larger scales (surface covered, node population…), or can be rather unpractical to set up on our platform. A cyber-physical simulator would allow overcoming the platform limitations and would open a wider spectrum of scenarios for security evaluation. These scenarios will be based on both real and simulated data, by adding for example a simulated rogue node in a scenario that has been recorded in real-life condition. Hence, the intern will implement cyber-physical simulation mechanisms within the existing 3D engine (written in Python), such as:

- Adding fictive tags to a previously recorded scenario.
- Introducing emulated rogue behaviors
- Generating random tags behaviors on a large scale.
- Detecting security violations
- Implementing system-level countermeasures in the simulated environment

The applicant should be enrolled in a Master degree in software engineering, computer science, embedded systems or equivalents.

Contact: baptiste.pestourie@lcis.grenoble-inp.fr
Skills: Python, C++, software engineering. Background in cybersecurity and embedded systems will be appreciated.

Stipend/Advantages*:* 530€/month + reduced-price in local cafeteria for lunch