Open Hardware Architecture for Safe and Secure IoT Systems

PhD proposal: Hardware Support For System Security

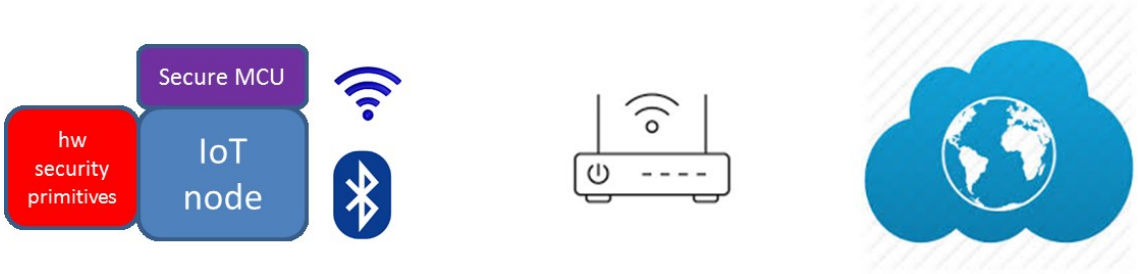
Context

The PhD will work within the framework of the European Project SERENE-(IoT Secured & EneRgy EfficieNt hEalth-care solutions for IoT market). *SERENE-IoT project is labelled within the framework of PENTA, the EUREKA cluster for Application and Technology Research in Europe on NanoElectronics.* SERENE_IoT project aims at contributing to develop high quality connected care services and diagnosis tools based on Advanced Smart Health-Care IoT devices, fully manufactured in Europe, enabling a good level of healthcare quality of service for patients remotely followed by professional caregivers, all at much lower cost than the traditional care provided today.

The main purpose of the LCIS task within the project is to focus on the processing unit of IoT devices dedicated to healthcare by developing an open platform which will allow to develop and to validate within the whole system:

1. Secure Processing Unit Architecture
2. Hardware support for system security features

Later on, the platform will be integrated within an IoT system with several connectivities (Lora, BLE). Global security schemes relying on low level security features embedded in the platform will then be developed and evaluated.



The PhD student will work on the development and validation of hardware based security mechanisms in order to securely integrate devices in safe and secure IoT systems. A first analysis of a given system will be done in order to point out the system weaknesses and to identify time and power consuming security dedicated task in order to finally integrate hardware security primitives which will be used to secure the system at the lowest cost (area/power/performance). Among other the device should:

- be authenticated by the system
- provide cryptographic services to insure confidentiality of communication (robust against side chanel attacks and fault attacks)
- provide secure storage of confidential data

  - manage different secure configuration and access credential through the device lifecycle
  - be isolated from the rest of the system in case of failure or malicious attack.
  - deal with blockchain

Many hardware features have been proposed within the literature in order to address the points discussed earlier. The PhD student will first have to reviews security needs and existing features quantifying the impact of each security features. Then, a system will be defined integrating existing or newly defined features with a demonstrator in order to build up higher level security policies based on these hw features.

- Necessary skills
  - Hardware design (digital IC design, knowledge of CMOS technology)
  - FPGA design
  - Embedded System prototyping (sw design to test the prototype or integrate the prototype in the system)
  - IoT Network knowledge (not mandatory)
  - Security

Contact:

David Hely (david.hely@lcis.grenoble-inp.fr) and Vincent Beroulle (vincent.beroulle@lcis.grenoble-inp.fr)