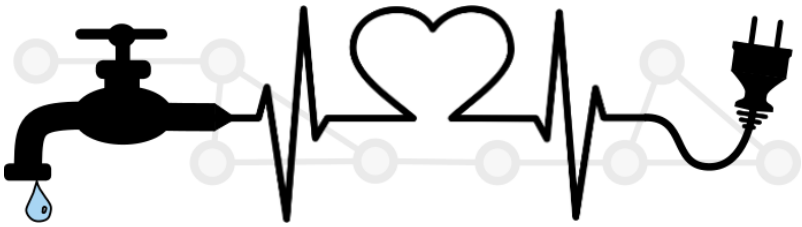
IoT: Information security in future critical infrastructures[1]



A quiet revolution that impacts several sectors, ranging over transport, home automation, energy, industrial control, and health services is undergoing with addition of new networked devices to obtain enhanced services. In our project we aimed to identify information security requirements common over several (vertical) sectors, and in particular, the ones that impact critical societal services. In order to assess the state in collaboration with industrial and societal partners we focused on three domains: the energy, water, and health management systems.

The work was initiated by organising workshops in which 4 stakeholders helped to identify the focus for a deeper analysis of security requirements in each domain. This resulted in formulated questions that were used in interviews with 14 actors in the three domains, with respondents ranging over different responsibility levels and backgrounds. Our final report summarises:

- findings from a literature review on the topic of IoT security, with a special focus on energy, water, and health management domains
- results of interviews with the 18 actors

These provide a picture of the gap between the current research outcomes and the perception of risks and vulnerabilities among the actors interviewed. A separate market study indicates that there is room for additional security-based services to enhance the provided security in the energy domain.

Our literature study reveals a number of novel threats in the IoT security ecosystem, and points out the lack of security building blocks that suit the specific low-resource requirements of IoT (e.g. limited memory, computation power, battery life time, and bandwidth). On the other hand, some security mechanisms that are hard to realise in a general IT network are easier to create in a critical infrastructure domain due to the restricted range of interaction possibilities and data transmissions. An example of such a building block is studied towards a proof of concept, namely an anomaly detector for a specific protocol running in data acquisition and supervisory control (SCADA) networks -- the IEC 60870-5-104 protocol.

Using data generated in an artificial but realistic test bed, the anomaly detection mechanism was evaluated with three unknown attacks. The results of the tests are promising and the study makes the possibility of tailor-made building blocks within a given SCADA domain concrete. The project report suggests avenues for future research in the new 5G era.

---

[1] Project contacts: Simin.Nadjm-Tehrani@liu.se , Mikael.Asplund@liu.se