Mission confiée

Scientific context

In last years, Internet-of-Things became a reality with numerous protocols, platforms and devices (8) being developed and used to support the growing deployment of smart* services: smart-home, - transport, - health, - city, and even the rather usual rigid systems with industry 4.0. Providing new services have required first the development of new functionalities with as underlining goals to have more power- and compute- efficient devices which can embed various sensors. Obviously, IoT also supposes a full infrastructure to guarantee the efficiency of communications and processing of the information. The embedded devices are thus completed by access points, routers, servers, etc. At the higher levels services are developed and provided to the users. This ecosystem is very rich and cannot be controlled by a unique entity, e.g services are often developed by third parties, manufacturer of embed devices are different to those providing connectivity... As a result, such a complex system is naturally a source of potential threats and realities recently demonstrated by naive weaknesses [1,6]. At Inria, we even demonstrated how simple and cheap can it be take over the control of a Z-Wave home installation in a silent manner [2].

Therefore, security is a paramount of importance in last model, many IoT architectures have been proposed, such as the reference model IoT-A [3], including security modules. However, as highlighted before, security cannot be guaranteed without failure or by-design and this is all the more true with evolving ecosystems such as IoT, with now the emerging trend of using fog-based architecture above than well-established cloud models. To enhance security, one option is to redesign an IoT architecture with stronger security but this will face the same problems as before, since some security issues can appear afterwards. Maintaining the architecture with new security elements would be therefore required but a remaining problems is the numerous number protocols or platforms that already exist. Nowadays, the only viable solution is to provide new security mechanisms that could be composed on demand and deployed in any IoT deployment by the operators, the integrators or the vendors rather than developing protocol- or architecture-centric security solutions.

- Missions: The main role of Inria in SecureIoT project is (6) to develop a security knowledge database to gather multiple sources of security information (such as those provided by MITRE corporation) and extend automatically knowledge with correlations and (2) define and implement the machine-learning based mechanisms for continuous security monitoring and predictive security of IoT systems.

At Inria, the research engineer will be involved in an expert team involving three researchers and one PhD student. The engineer will work in close collaboration with them participating so in the design of solutions for the security of IoT and their implementation.

- Bibliography:

[5] BF Van Dongen et al., The prom framework: A new era in process mining tool support, ICAITP 2005

Contexte et atouts du poste

The offered position is in the context of SecureIoT SecureIoT is a European project (https://secureiot.eu/) and a joint effort of global leaders in IoT services and IoT cybersecurity to secure the next generation of dynamic, decentralized IoT systems, that span multiple IoT platforms and networks of smart objects, through implementing a range of predictive IoT security services. The project integrates its security services in three different application scenarios in the areas of: Digital Automation in Manufacturing (Industry 4.0), Socially assistive robots and IoT security services. SecureIoT will integrate its security services in three different application scenarios in the areas of: Digital Automation in Manufacturing (Industry 4.0), Socially assistive robots and Embedded systems.

Principales activités

- Definition of a security knowledge base: the objective is to define and develop all the interfaces and probes to collect identified sources of information (can be attacks, vulnerabilities, threats) to be consolidated in to a single database. The definition of the database includes the selection of technologies to be used and the data representation. In addition, the engineer will be in charge of integrating algorithms produced by researchers aiming at automatically make additional correlations among entities in the database.

- Development of analytics module for monitoring and predictive security. This will be in close evolving and strong collaborations with Inria researchers and the PhD student working on machine learning techniques. This task will consist in properly integrating developed algorithms in the SecureIoT project platforms as for example by developing necessary probes or interface to collect necessary input data and support other decisions modules with the results.
Project management. The research engineer will be fully involved in the project management duties including writing and reviewing of deliverables of the project; participating to the project meetings, including physical meetings being held in different countries of Europe; management of tasks involving multiple partners (for example, other partners will also integrate algorithms in the platform).

Compétences
- Required qualification: Diplôme d'Ingénieur, Master degree in Computer Science or Computer engineering
- Languages: Java, python and others are appreciated
- Database and big data technologies: SQL and NoSQL, MongoDB, TinkerPop, Spark, Apache
- Software development: continuous integration and collaborative development using gitlab, knowledge in virtualisation technologies (containers with Docker)
- Knowledge in machine learning and data mining
- Fluent in English (writing and oral communication)
- Comfortable with meetings and webconference situations

Avantages sociaux
- Subsidised catering service
- Partially-reimbursed public transport
- Social security
- Paid leave
- Flexible working hours
- Sports facilities

Rémunération
Monthly gross salary from 2562,00€