2019-01242 - Temporary scientific engineer / Software development and machine learning for network security

Contrat renouvelable : Oui
Niveau de diplôme exigé : Bac + 5 ou équivalent
Fonction : Ingénieur scientifique contractuel

Contest et atouts du poste

- **Scientific Context:** In last years, Internet-of-Things became a reality with numerous protocols, platforms and devices that were 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 in these areas requires the development of new functionalities with as underlying 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 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 end-to-end architecture cannot be controlled by a unique entity, e.g. services are often developed by third parties, manufacturer of embedded devices are different to those providing connectivity. As a result, such a complex system is notably a source of potential threats and real cases recently demonstrates that IoT can be affected by naive weaknesses [1,6]. At Inria, we even demonstrated how simple and cheap it can be take over the control of a Z-Wave home installation in a silent manner [2]. Therefore, security is paramount and important. In last decade, 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 rather 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.

- **Project context:** SecureIoT is a European project (http://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. 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 robots for healthcare and Connected cars and Autonomous Driving.

Mission confiée

- **Project context:** SecureIoT is a European project (http://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. 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 robots for healthcare and Connected cars and Autonomous Driving.

- **Role of the engineer**
  - The recruited engineer will have to support researchers, including junior researchers (PhD student) in the software development and integration of data analytics techniques, refine probes (i.e. for collectors) and integrate them within the given project architecture (Logstash, Elasticsearch, Spark, Kafka) and write/review technical documents.

Principales activités

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 in so in the design of solutions for the security of IoT and their implementation. More specifically, he or she will be in charge of the following tasks:

- Implementation and integration of a security knowledge base containing cyber threat intelligence information; the objective is to define and develop all the interfaces and probes to collect identified sources of information (about attacks, vulnerabilities, threats) to be consolidated in to a single database. The current implementation relies on OrientDB, MongoDB and TinkerPop. The engineer will be in charge of updating the implementation and the integration within the project including the addition of new data sources to be crawled/queried and integrated (for example MISP - http://www.misp-project.org/) and the development of necessary interfaces with other components and using continuous integration with gitlab and docker.
Development of analytics module for monitoring and predictive security. This will be in close 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, reviewing and editing of deliverables of the project; participating to the project meetings, including physical meetings being held in different countries of Europe and review meetings; management of tasks and a workpackage involving multiple partners.

Compétences
- Skills and profile:
  - 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
- Subsidised catering service
- Partially-reimbursed public transport
- Social security
- Paid leave
- Flexible working hours

Rémunération
Monthly gross salary from 2562,00€