in charge of the following tasks:

At Inria, the research engineer will be involved in an expert team involving three researchers and one software developer to implement and develop new functionalities with an underlying goal of having 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 development 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 demonstrate that IoT can be affected by naive weaknesses [1,6]. At Inria, we have demonstrated how simple and cheap it can be to 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 new threats emerging. To design an IoT architecture with strong security but this will face the same problems as before, since some security issues can appear afterwards. Maintaining the architecture with new security elements will be therefore required but a remaining problem is the numerous number of 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.


Mission confiée

- Project context: SecureIoT is a European project (http://secureiot.eu) and a joint effort of global leaders in IoT-sever security 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 for coaching and healthcare and Connected cars and Autonomous Driving. The main role of Inria in this project is (1) to develop a security knowledge database to gather multiple sources of security information (as such as those provided by MITRE corporation) and extend automatically by correlations and (2) define and implement the machine-learning based mechanisms for continuous security monitoring and predictive security of IoT systems.

- 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 collecting/processing network traffic in IoT) and integrate them within the given project architecture (Logstash, Elasticsearch, Spark, Kafka) and write/review technical documentation.

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 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 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.

Informations générales

- Thème/Domaine : Réseaux et télécommunications
- Ingénierie logicielle (BAP E)
- Ville : Villennes-sur-Seine
- Centre Inria : CRI Nancy - Grand Est
- Date de prise de fonction souhaitée : 2019-05-01
- Durée de contrat : 1 an
- Date limite pour postuler : 2019-03-11

Contacts

- Equipe Inria : RESIST
- Recruteur : François Jérôme / jerome.francisco@inria.fr

À propos d’Inria

Inria, l’institut national de recherche dédié aux sciences du numérique, promeut l’excellence scientifique et le transfert pour avoir le plus grand impact. Il emploie 2400 personnes. Ses 200 équipes-projets agiles, en général communes avec des partenaires académiques, impliquent plus de 3000 scientifiques pour relever des défis des sciences informatiques et mathématiques, souvent à l’interface d’autres disciplines. Inria travaille avec de nombreuses entreprises et a accompagné la création de plus de 160 start-up. L’institut s'efforce ainsi de répondre aux enjeux de la transformation numérique de la science, de la société et de l'économie.

Consignes pour postuler

Sécurité défense :

Ce poste est susceptible d’être affecté dans une zone à régime restrictif (ZRR), telle que définie dans le décret n°2011-1425 relatif à la protection du potentiel scientifique et technique de la nation (PPST). L’autorisation d’accès à une zone est délivrée par le chef d’établissement, après avis ministériel favorable, tel que défini dans l’arrêté du 03 juillet 2012, relatif à la PPST Un avis ministériel défavorable pour un poste affecté dans une ZRR aurait pour conséquence l’annulation du recrutement.

Politique de recrutement :

Dans le cadre de sa politique diversité, tous les postes Inria sont accessibles aux personnes en situation de handicap.

Attention : Les candidatures doivent être déposées en ligne sur le site Inria. Le traitement des candidatures adressées par d’autres canaux n’est pas garanti.
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 sociaux

- Subsidised catering service
- Partially-reimbursed public transport
- Social security
- Paid leave
- Flexible working hours

Rémunération

Monthly gross salary from 2562,00€