2018–00302 - [INDES] Design and enforcement of user's privacy policies in IoT applications

Niveau de diplôme exigé : Bac + 5 ou équivalent
Fonction : Doctorant

A propos du centre ou de la direction fonctionnelle

The Inria Sophia Antipolis - Méditerranée center counts 37 research teams and 9 support departments. The center's staff (about 600 people including 400 Inria employees) is composed of scientists of different nationalities (250 foreigners of 50 nationalities), engineers, technicians and administrators. 1/3 of the staff are civil servants, the others are contractual. The majority of the research teams at the center are located in Sophia Antipolis and Nice in the Alpes-Maritimes. Six teams are based in Montpellier and a team is hosted by the computer science department of the University of Bologna in Italy. The Center is a member of the University and Institution Community (ComUE) “Université Côte d’Azur (UCA)”.

Contexte et atouts du poste

The CISC “Certification of IoT Secure Compilation” project, which is funded by ANR, the French National Research Agency, aims to investigate multitier languages and compilers to build secure IoT applications with privacy guarantees. The goal of the project is to define language, semantics, attacker models, and policies for the IoT and investigate the automatic implementation of privacy and security policies. The consortium includes 10 researchers and professors from all over France. This job description concerns one of the open positions within this project.

Mission confiée

The Techbeacon report (April 2016) states that 90% of the most commonly used IoT devices collect at least one piece of personal information. Moreover, 80% of them raise privacy concerns. IoT systems process a vast amount of user's data that gets collected through a variety of devices such as sensors, beacons and mobile phones. Therefore ensuring that these systems comply with privacy rights and regulations is a main challenge.

Various languages and frameworks have been proposed to express privacy policies but they are not necessarily well suited to the IoT [1, 2]. One major requirement in the next generation IoT applications is user's consent, which plays the key role in the upcoming EU privacy regulations, such as General Data Protection Regulation (GDPR) [3] and ePrivacy [4]. To be legitimate from a legal point of view, user's consent must be free, specific, informed and unambiguous. The existing privacy policy languages are often too coarse-grained: they don't provide functionality to express consent, and may force users to disclose more data or grant third parties broader rights than they would like. In addition, they do not take into account the specificities of the IoT (variety of small devices with scarce resources, sometimes working in a passive mode, etc.).

Citations:

[3] Regulation (eu) 2016/679 of the european parliament and of the council 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation).
[4] Proposal for a Regulation on Privacy and Electronic Communications of 10 January

Principales activités

We aim to address the above mentioned issue with an innovative approach, and develop a user-friendly language to express privacy policies and then automatically enforce them in IoT applications. The three main tasks of this PhD thesis will be:

1) Definition of a privacy policy language — we will take into account three essential requirements that have not been jointly addressed in a satisfactory manner so far: suitability to the IoT, user-
friendliness and formal semantics.

2) Translation of user-defined privacy policies into enforceable policies — in addition to being understandable by users, policies should therefore be translatable into machine-readable policies and applied to the corresponding data.

3) Enforcement of privacy policies by certified compilation — adapting the machine-readable policies to a multitier compiler (developed in the project, based on [5, 6]) that transforms an IoT application into an application where all the required policies are properly integrated.

Collaboration:

The PhD student will closely work within the INDES research team of the Sophia-Antipolis Inria Research Center with strong interactions with PRIVATICS team (in Lyon and Grenoble, Rhône-Alpes Inria Research Center) and the CELTIQUE team (in Rennes, Bretagne Inria Research Center).

Citations:


Compétences

Master degree in Computer Science or Computer Engineering is required. Programming skills. Knowledge of Formal Semantics and program analysis is preferred. Fluent English required, both oral and written.

Knowledge of French is not required.

Avantages sociaux

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

Rémunération

Duration: 36 months
Location: Sophia Antipolis, France
Gross Salary per month: 1982€ brut per month (year 1 & 2) and 2085€ brut/month (year 3)