that have not been jointly addressed in a satisfactory manner so far: suitability to the IoT, user-friendly language to express privacy policies and then automatically enforce them in IoT applications.

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: the 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.).

2) Design of a privacy policy language for IoT — 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.).

3) Automatic enforcement of privacy policies — we will develop a system to automatically enforce privacy policies in IoT applications.

Citations:

[4] Proposal for a Regulation on Privacy and Electronic Communications of 10 January

Principal activities

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-friendly language to express privacy policies and then automatically enforce them in IoT applications.

2) Design of a privacy policy language for IoT — 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.).

3) Automatic enforcement of privacy policies — we will develop a system to automatically enforce privacy policies in IoT applications.

Informations générales

- Thème/Domaine: Programmation distribuée et génie logiciel
- Développement web (BAP E)
- Ville: Sophia Antipolis
- Centre Inria: CRI Sophia Antipolis - Méditerranée
- Date de prise de fonction souhaitée: 01-09-2018
- Durée de contrat: 3 ans
- Date limite pour postuler: 31-07-2018

Contacts

- Equipe Inria: INDES
- Recruteur: Bielova Nataliia / nataliia.bielova@inria.fr

Conditions pour postuler

Application file: Applications must be submitted online on the Inria website. Collecting applications by other channels is not guaranteed.

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.
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)