2018-00917 - Usage control for personal data: using isolation techniques to regulate data sharing in a personal cloud context

Level of qualifications required: Graduate degree or equivalent
Function: PhD Position

About the research centre or Inria department
Located at the heart of the main national research and higher education cluster, member of the Université Paris Saclay, a major actor in the French Investments for the Future Programme (Idex, LabEx, IRT, Equipe) and partner of the main establishments present on the plateau, the centre is particularly active in three major areas: data and knowledge, safety, security and reliability; modelling, simulation and optimisation (with priority given to energy).

The 450 researchers and engineers from Inria and its partners who work in the research centre's 31 teams, the 100 research support staff members, the high-level equipment at their disposal (image walls, high-performance computing clusters, sensor networks), and the privileged relationships with prestigious industrial partners, all make Inria Saclay Île-de-France a key research centre in the local landscape and one that is oriented towards Europe and the world.

Assignment
The Personal Cloud paradigm holds the promise of a Privacy-by-Design storage and computing platform, where each individual can gather her complete digital environment in one place and share it with applications and users, while preserving her control. However, this paradigm leaves the privacy and security issues in users' hands, which leads to a paradox if we consider the weaknesses of individuals' autonomy in terms of computer security, ability and willingness to administer sharing policies. The challenge is however paramount in a society where emerging economic models are all based - directly or indirectly - on exploiting personal data.

While many research works tackle the organization of the user's workspace, the semantic unification of personal information, the personal data analytics problems, the objective of the PETRUS project-team is to tackle the privacy and security challenges from an architectural point of view. More precisely, the objective of this PhD is to propose new data administration model reaching the main requirements of a personal cloud (decentralized access and usage control models, data sharing, data collection and retention models, etc.) and study the enforcement of the resulting privacy policies based on the introduction of trusted and isolated execution environment.

A preliminary architectural contribution, called SWYSWYK, has recently been proposed by the team, and will serve as a starting point for this PhD. More specifically, a first objective will be to derive from this work a sufficiently formalized architecture, based on properly defined security properties, to build security evidence of the resulting system. In a second step, a more elaborate model of control of use will be investigated, allowing the user to declassify his data and to make informed decisions concerning the sharing without difficulty.

Main activities
The goal of this thesis is to design a personal cloud architecture that allows users to control the sharing and uses of their personal data, minimizing accidental or malicious disclosures that may occur.

The initial idea is to consider a 2-level architecture: (1) a monitor capable of responding to simple authorization requests (minimization of the code) considered to be trusted, on which could be grafted (2) more complex modules having access to the user's raw data and to usage logs (e.g., actual access to data) allowing to construct authorized views of the complex data and recommendations as to the use and sharing of this derived information.

The thesis will be co-supervised by Nicolas Anciaux and Guillaume Scerri, in the PETRUS team.

Bibliographical references:
- Manuel Barbosa, Bernardo Portela, Guillaume Scerri, Bogdan Warinschi. Foundations of Hardware-Based Attested Computation and Application to SGX. EuroSSP, 2016

Skills
The successful applicant will have a masters (or any equivalent degree) in computer science. He will have a strong background both in computer security and databases. A knowledge of cryptography and/or formal methods would be a plus.

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

Monthly gross salary: 1.982 euros 1st and 2nd year
Monthly gross salary: 2.085 euros 3rd year