A propos du centre ou de la direction fonctionnelle

The Inria Saclay-Île-de-France Research Centre was established in 2008. It has developed as part of the Saclay site in partnership with Paris-Saclay University and with the Institut Polytechnique de Paris.

The centre has 34 project teams, 27 of which operate jointly with Paris-Saclay University (15 teams) and the Institut Polytechnique de Paris (12 teams). Its activities occupy over 600 people, scientists and research and innovation support staff, including 44 different nationalities.

The centre also hosts the Institut DATIA , dedicated to data sciences and their disciplinary and application interfaces.

Contexte et atouts du poste

This thesis takes place within the framework of the PEPR (Priority Research Program and Equipment) Cybersecurity iPoP (interdisciplinary Project on Privacy) project involving several internationally recognized French research teams working on data protection, from universities, engineering schools and national research organizations, as well as the CNIL (French National Commission on Information Technology and Civil Liberties).

Mission confiée

Context. The PETRUS team designs and implements decentralized personal data management techniques for the individual, with the ambition to allow users to manage their data for their personal use and to collectively contribute to statistical calculations with their data, while ensuring data confidentiality, the integrity of the calculation performed, and the minimization of data exposure in case of attack, all this in accordance with the new European general data protection regulation (GDPR). To this end, the team proposes new architectures and secure computing techniques [1]. These proposals are based on the hypothesis of personal computing devices, called PDMS (Personal Data Management System), equipped with secure hardware (e.g., current Intel processors that integrate “Software Guard Extensions” (SGX), AMD processors equipped with a “Platform Security Processor” (PSP), ARM processors equipped with TrustZone, etc.) Such hardware is now present on most existing platforms. It offers primitives for protecting data and code from the execution environment (including the operating system) running on the host machine.

Objectives of the thesis. The PDMS approach leads to a major paradigm shift because the processing of the user’s data is done in their PDMS. However, this is not enough to guarantee the security of the processing. The objective of this thesis is to design and implement strategies for executing computations on personal data in a PDMS (e.g., statistical computations on time series data, e.g., GPS traces or power consumption traces). These strategies must guarantee an upper bound on leakage (e.g., quantifiable according to the type of computation or data) while ensuring the efficiency of the treatments. To address this problem, we use an architectural model [1] that relies on the execution of a trusted enclave (called Core) as well as processing enclaves (called Data Tasks) on which no security assumptions are made (i.e., potentially malicious). Data Tasks are executed under constraints (e.g., without allowing to maintain a state between successive executions [2], without having access to random sources) and under the supervision of the Core in order to guarantee a minimal data leakage in case of malicious code execution within the PDMS [3]. Another challenging related problem is data indexing considering this architecture and its constraints. The classical approach which considers the index code as part of the trusted computing base (e.g., see [4]) cannot systematically be apply in the PDMS context. That is, the indexing methods can only exceptionally be part of the Core and have to be implemented as Data Tasks in general. This also leads to a tension between the leakage risk with untrusted indexing code and indexing efficiency. Currently, the PETRUS team is designing a prototype PDMS on an Intel SGX platform [3] based on the execution of code within SGX enclaves and this prototype can be used in this thesis.

References.


state of the art of data management within Trusted Execution Environments
- design and implement strategies for executing computations on personal data
- write and present research papers

Compétences
Technical skills and level required:

Languages:

Relational skills:

Other valued appreciated:

Avantages
Subsidized meals
- Partial reimbursement of public transport costs
- Leave: 7 weeks of annual leave + 10 extra days off due to RTT (statutory reduction in working hours) + possibility of exceptional leave (sick children, moving home, etc.)
- Possibility of teleworking (after 6 months of employment) and flexible organization of working hours
- Professional equipment available (videoconferencing, loan of computer equipment, etc.)
- Social, cultural and sports events and activities
- Access to vocational training
- Social security coverage

Rémunération
First and second year: 2,051 euros/month
Third year: 2,158 euros/month

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.