2018-00903 - Doctorant / Sécurisation de traitement orientés données à base d'environnement d'exécution de confiance

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, Plateformes), the CRI Saclay - Île-de-France is a key research centre in the local landscape and one that is oriented towards Europe and the world.

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 context, because of data protection mechanisms, access to RAM is much more expensive. This leads directly or indirectly - on exploiting personal data.

Two different issues have to be considered here. The first one is how the specific memory architecture of SGX affects classical data processing algorithms. The second objective of this internship is to evaluate the second issue is understanding how side channel attacks on SGX (timing, memory access patterns) affects classical data processing algorithms in the context of computer security. The challenge is however paramount in a society where emerging economic models are all based on exploiting personal data.

On the other hand, trusted execution environments (TEE), like Intel SGX, are now embedded in end-users' personal computers and in cloud servers. From a security point of view, it offers the capabilities to run code in isolation and provide remote attestations, which allows to prove required properties of the code running to third parties. Additionally, TEEs provide mechanisms for managing the information flow from code running in the TEE to the outside world, secure external storage thanks to encryption, and manage the communications between different processes running in a TEE. Typically, Intel SGX integrates cryptographic primitives in hardware, with an impact on the performance of data oriented tasks which remains to analyze.

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 team is to tackle the privacy and security challenges from an architectural point of view. This PhD will investigate the design of database structures and algorithms in trusted execution environments for the personal cloud context.

Assignment

The goal of the PhD are (i) to identify the specific constraints of trusted execution environments (e.g., Intel SGX) with respect to personal database management tasks and understand how side channel attacks on trusted execution environments (timing, memory access patterns) affect classical data processing; and (ii) to propose appropriate design rules for data structures, algorithms and counter measures, for efficient, scalable and secure personal data management using secure enclaves.

Main activities

The Intel SGX technology is embedded in all recent Intel CPUs present in personal computers and cloud servers. From a security point of view, it provides a trusted execution environment (TEE), called enclave in the SGX context. More precisely, it offers the capabilities to run code in isolation and provide remote attestations, which allows to prove required properties of the code running to third parties.

Additionally, TEEs provide mechanisms for managing the information flow from code running in the TEE to the outside world, secure external storage thanks to encryption, and manage the communications between different processes running in a TEE. Intel SGX therefore integrates cryptographic primitives in hardware, with an impact on the performance of data oriented tasks which remains to analyze.

In the PETRUS team, we use Intel SGX to secure data computations preformed in a personal cloud context. More precisely, our goal is to process data under the control of the user either on the user's SGX enabled machine or in an untrusted cloud context using the SGX attestation mechanism. In this context, SGX provides an invaluable building block as it allows to isolate tasks from the – potentially compromised – user OS, or the untrusted cloud owner infrastructure, thus allowing for strong security guarantees against a realistic adversary that might compromise the user machine through malware, and compromise security of a cloud provider (either through an insider attack or a large scale compromise as seen recently). The aim of this internship is to identify tradeoffs between efficiency and security that have to be made when securing data processing tasks using SGX. This is an essential issue as the security and computation model of SGX are rather far from the well studied case of on dedicated processing server.

Two different issues have to be considered here. The first one is how the specific memory architecture of SGX affects the data management tasks. Indeed, SGX has two important limitations: first, the amount of protected memory is rather limited (roughly 100 Mo) compared to modern unprotcted systems; second, while access to CPU cache from an enclave is similar to an unprotected context, because of data protection mechanisms, access to RAM is much more expensive. This leads to the first objective of this internship: benchmarking data processing tasks in the context of SGX in order to understand which algorithms are well suited for data processing in this context. The second issue is understanding how side channel attacks on SGX (timing, memory access patterns) affects classical data processing algorithms. The second objective of this internship is to evaluate the impact of these attacks on data processing tasks protected in enclaves and devising counter measures to protect against these attacks.
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
1st and 2nd year gross salary: 1,982 euros/month
3rd year gross salary: 2,085 euros/month