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. 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 challenge is however paramount in a society where emerging economic models are all based - directly or indirectly - on exploiting personal data.

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 perform advanced data oriented computations on her data with strong privacy and security guarantees. However, this paradigm leaves the privacy and security issues in users' hands, which leads to a paradox if we consider the whole environment in terms of computer security.

The second issue is understanding how side channel attacks on SGX (timing, memory access patterns) affect classical data processing tasks protected in enclaves and devising countermeasures to protect against these attacks.

Context

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. 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. Typically, Intel SGX 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 performed 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 unprotected 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 the data processing tasks in the context of SGX. To this end, 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.

About Inria

Inria, the French National Institute for computer science and applied mathematics, promotes "scientific excellence for technology transfer and society". Graduates from the world's top universities, Inria's 2,000 employees rise to the challenges of digital sciences. With its open, agile model, Inria is able to explore original approaches with its partners in industry and academia and provide an efficient response to the multidisciplinary and application challenges of the digital transformation. Inria is the source of many innovations that add value and create jobs.

Conditions for application

Defence Security:

This position is likely to be situated in a restricted area (ZRR), as defined in Decree No. 2011-1425 relating to the protection of national scientific and technical potential (PPST). Authorisation to enter an area is granted by the director of the unit, following a favourable Ministerial decision, as defined in the decree of 3 July 2012 relating to the PPST. An unfavourable Ministerial decision in respect of a position situated in a ZRR would result in the cancellation of the appointment.

Recruitment Policy:

As part of its diversity policy, all Inria positions are accessible to people with disabilities.

Warning: you must enter your e-mail address in order to save your application to Inria. Applications must be submitted online on the Inria website. Processing of applications sent from other channels is not guaranteed.
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