



Language-level Support for Software Development with Intel SGX

HiWi Position

Data privacy is a major concern in the design of distributed systems where data is processed by different machines that are not necessarily under the control of the same user. In this setting, there is a concrete possibility of private data leaks which, e.g., in the case of medical data, can lead to catastrophic consequences. Unfortunately, traditional security measures such as access control and application layer cryptography are not always sufficient to protect against attacks that compromise data privacy.

Intel SGX [1] is a recent technology to define a private computing environment that provides strong protection against high privilege attacks.

Goal:

This work involves developing a programming model in a high-level language such as Java (or Scala) that can efficiently support computations in SGX environment. The programming model will be tested for performance and security by implementing suitable test cases.

Prerequisites:

Java programming, familiarity with Linux/macOS

Keywords: Java, Scala, SGX

References:

[1] <https://software.intel.com/sites/default/files/managed/33/70/intel-sgx-developer-guide.pdf>

Contact:

Prof. Dr. Guido Salvaneschi

S2|02 B218