4 Analysis of existing technologies

This chapter discusses approaches to increase security of data processing in untrusted environments. We will discuss three well-known approaches, namely, Intel Software Guard Extensions, trusted and secure boot, and secure computation.

4.1 Intel SGX

Intel **S**oftware **G**uard e**X**tensions (SGX) is an Intel hardware-based technology for ensuring security of sensitive data from disclosure or modification. It enables user-level code to allocate enclaves (i.e., private regions of memory) that are protected even from processes running at higher privilege levels. Intel SGX capabilities are available from a set of instructions introduced in off-the-shelf processors, starting from the 6th Generation Intel Core family, based on the Skylake microarchitecture.

4.1.1 Components

The application of the Intel SGX technology requires four main componentes: (i) the availability of the set of instructions in the processor, (ii) the operating system driver, (iii) the software development kit to facilitate the access to the driver from the application code, and (iv) Platform Software.

The *Platform Software* (**Intel SGX PSW**) is a collection of special SGX enclaves, and an Intel SGX Application Enclave Services Manager (**AESM**), provided along with the SGX SDK. These special enclaves and AESM are used when loading enclaves, retrieving cryptographic keys, and evaluating the contents of an enclave. The *software development kit* (**SDK**) is a collection of APIs, sample source code, libraries and tools that enable software developers to write and debug SGX applications in C/C++. Next, the *drivers* enable OS's and other software to access the SGX hardware. Intel SGX drivers are available both for Windows (via Intel Management Engine) and for Linux* OS's. Finally, the *instruction set* is composed of 17 new instructions that can be classified into the following functions [54]:

Enclave build/teardown: Used to allocate protected memory for the enclave, load values into the protected memory, measure the values loaded into the enclave's protected memory, and teardown the enclave after the application has completed. Instructions used for this purpose are:

- ECREATE - Declare base and range, start build
- EADD - Add 4k page
- EEXTEND - Measure 256 bytes
- EINIT - Declare enclave built
- EREMOVE - Remove Page

Enclave entry/exit: Used to enter and exit the enclave. An enclave can be entered and exited explicitly. It may also be exited asynchronously due to interrupts or exceptions. In the case of asynchronous exits, the hardware will save all secrets inside the enclave, scrub secrets from registers, and return to external program flow. It then resumes where it left off execution. Instructions used for this purpose are:

- EENTER - Enter enclave
- ERESUME - Resume enclave
- EEXIT - Leave enclave