IST 597 Project Report Wrapper

Yufei Jiang

1 The Difference between Intel SGX and ARM TrustZone

1.1 Overview

Trusted Computing (TC) is a concept developed by the Trusted Computing Group. It has been discussed for years. Regarding the meaning of "trusted", there are a lot of controversy. Some people also challenge the idea of Trusted Computing fundamentally since it may be harmful to keep anonymity over Internet and avoid vendor-lock-in. Despite the buzz, some players in the technical industry, including Dell, HP, Microsoft, Intel, and ARM have made solid progress on realizing this concept.

In this report, we will investigate two concrete Trusted Computing solutions. They are Intel SGX and ARM TrustZone. According to the definitions given by Trusted Computing Group. A complete Trusted system must have the following 6 elements: endorsement key, secure input and output, memory curtaining, sealed storage, remote attestation, and trusted third party. More specifically, both Intel SGX and ARM TrustZone are two measurements to fulfill some parts in the whole Trusted system.

In the following subsections, we will first briefly introduce Intel SGX and ARM TrustZone respectively. Then we will compare them two from certain aspects.

1.2 Intel SGX

The full name of Intel SGX is Intel Software Guard Extensions. Intel SGX is a technology to help developers better protect the confidentiality and integrity of selected code and data of their applications from those rogue software that is running in higher level including the operating system. It was implemented in 6th generation Intel Core microprocessors in 2015 for the first time. Its basic mechanism is to create some protected areas in memory which are called "enclaves". Developers can explicitly use Intel SGX SDK during the development to put the data and code of interests into enclaves.

1.3 ARM TrustZone

According to ARM, ARM TrustZone technology "is a System on Chip (SoC) and CPU system-wide approach to security". Its key idea is to provide two virtual processors to create two hardware-separated worlds, the secure world and the insecure world. Any information flows from the secure world to the insecure world must go through the secure monitor. Besides this difference, the two worlds have the same capabilities so each side can operate independently.

1.4 Comparison

1.4.1 Architecture

Both Intel SGX and ARM TrustZone are security extensions to their existing CPU architectures. Conceptually, Intel SGX is more lightweight than ARM TrustZone. Intel SGX essentially is an extension to Intel instruction sets. Only with those special instructions, data can be read from written to the enclaves. ARM TrustZone, from our point of view, is a hardware-assisted virtualization. It provides two completely separate virtual running environment. Each side has the complete computation capacity. To this extent, Intel SGX and ARM TrustZone have different security models.

1.4.2 Security

Intel SGX and ARM TrustZone follows the different security models. The security provided by Intel SGX are from following two aspects. First, only several specific instructions, which requires explicitly to be called by developers, can access enclaves. Second, the cryptographic key is only available to the Intel processors. In short, Intel SGX tries to help developers to achieve information hiding. ARM TrustZone, from our perspective, provides isolation, which does not grant security automatically. The key insights of ARM TrustZone are to reduce attack surface and isolation. It assumes that developers will put almost all code in the insecure world. Those code, such as the operating system, is complex, hard to be audited and analysed. They are doomed to have exploitable vulnerabilities. On the other hand, even the secure world has the capability of running any code, we usually only put some small pieces of code in the secure world. Those code has simpler logic and performs some critical function, like signing or making a transaction. So we can review, audit, perform model checking, analyze those code to make sure it is very likely to be bug free. A malicious user may temper the operating system in the insecure world easily, however, he still cannot perform those critical functions in the secure world arbitrarily. However, if the code in the secure world has vulnerabilities, TrustZone cannot prevent a malicious user from exploiting it.

1.4.3 Development

Development in Intel SGX is easier. Intel SGX provides enclave binding API in C and C++. To utilize Intel SGX in an application, a developer can use the API provided by Intel SGX SDK. A developer can explicitly put the data of interests into enclaves. The two most important APIs are for creating and destroying enclaves in the memory. Conceptually, they are just like special "malloc" and "free".

Regarding ARM TrustZone,

1.4.4 Invocation

During runtime, the SGX APIs called by the application will invoke the driver of SGX to perform encryption, decryption, read, and write operations. In ARM TrustZone, when the insecure world requests a service in the secure world, it makes a SMC call to transfer the control to the secure world.

1.4.5 Encryption

Intel SGX uses symmetric encryption to encrypt the data in enclaves. The key will be refreshed in every boot. ARM TrustZone, on the other hand, does not encrypt the data in the secure world, since it follows a different security model.

1.4.6 Adoption

Intel SGX is different from ARM TrustZone. Architecturally, with ARM TrustZone, a CPU is in two halves which are insecure world and the secure world. Any communication occurs from the insecure world to the secure world is via the Secure Monitor Call (SMC) instruction. At the meanwhile, in Intel SGX model, there is only one CPU with many secure enclaves. Conceptually, Intel SGX is similar to "Protected Process" which is implemented in Microsoft Windows Vista for the first time. However, Intel SGX is safer since it is enforced by hardware.

Regarding ARM TrustZone, ARM is historically associated with so called "single- purpose systems". The System on Chip (SoC) is customized to some specific markets (e.g. smartphones) so there is only one "Trust Zone". Intel SGX has multiple enclaves in a system. So it can be used in a more general multi-purpose chips.

Test [1]

References

[1] "Church encoding," http://goo.gl/I03nLI, accessed: 2015-04-22.