

# Research Report for Secure EL2

Shiqing Liu

South University of Science and Technology  
Shenzhen, China

Email: liusq2017@mail.sustech.edu.cn

Yinhua Chen

South University of Science and Technology  
Shenzhen, China

Email: homer@thesimpsons.com

**Abstract**—The abstract goes here.

## I. INTRODUCTION

Trusted Execution Environment (TEE) is a domain in CPU who is isolated from TEE.

History of TEE.

History of virtualization.

History of virtualizing TEE.

Basic idea to virtualize TEE.

Virtualized TEE in industry. Sierraware. Imagination Technologies

The arrangement of the report. Firstly talk about the software-simulation base virtualization(vTZ). second hardware-assisted base virtualization(not SEL2)

## II. HYPERVISOR

Some

## III. SOFTWARE SIMULATION BASED TEE VIRTUALIZATION(?)

The software simulation base TEE virtualization is to create a virtual TEE and simulate a part of, even all of TEE functionalities in a software way. The important component of TEE, such as interrupt controller and memory controller, is achieved by the software. The representative is vTZ.

### A. vTZ

vTZ is proposed by Zhichao Hua in 2017 on usenix conference. TrustZone does not provide any hardware support for virtualization at that time. All VMs in normal world should share the same TEE and it leads to a serious security issue for breaking the isolation of VMs. vTZ aims to virtualize TrustZone and provide each VM an independent TEE. Different from other jobs, it makes use of the existing TEE architecture instead of designing a new one. vTZ separates the functionality and security by running another VM in normal world as guest TEE to serve the VM. The security is ensured by the TrustZone hardware isolation. In details, a tiny monitor in secure world controls the memory mapping and world switching. A Constrained Isolated Execution Environment (CIEE) provides isolation.

The design of vTZ is shown in figure. There are four secure modules in vTZ, Secure Memory Mapping (SMM), Secure World Switching (SWS), Control Flow Lock (CFLock), and Constrained Isolated Execution Environment (CIEE). Running

in secure world, SMM controls all memory mappings. To achieve that, the hypervisor is not allowed to contain the sensitive instruction to access and control the translation table, not to mention the first level translation and second level translation. Instead, the sensitive instruction is replaced by the invocation to SMM. SMM will check whether the request is legal. SWS is responsible for the world switching and it is another module in secure world. It will check the VID of the VMs and restore the correct VM. As long as SWS ensures the correctness of the switch from VMs to the hypervisor and the hypervisor to VMs, all switches in vTZ will be covered, because switches between VMs are composed of both switches. As a module in normal world hypervisor, CFLock is used to prevent the execution control flow from tempering by protecting exception vector table. CFLock can be used to ensure SWS will eventually handle all switches. The last module is CIEE, a region in normal world EL2, running with the hypervisor, serves the guest-TEE. CIEEs contain the software implementations of TrustZone. In other words, vTZ does not utilize all the hardware in consideration of the support of the virtualization. To protect the isolation and security of CIEE, CIEE is designed to execute atomically and independently. The CIEE itself is also verifiable. As a result of it, CIEE can't be falsified.

Based on these four modules, vTZ reaches the goal of secure boot, memory isolation, and privilege isolation.

The advantages of vTZ are high efficiency and high security. In vTZ evaluation, the performance overhead of applications is low compared to the native environment, TrustZone, and Xen hypervisor. For security, vTZ has a TCB of thousands of lines of code, which is far less than one who puts an entire hypervisor and guest TEE into secure world. And vTZ utilizes TrustZone to protect itself. In details, the privilege mode and secure world of TrustZone make the isolation and security of CIEE, SWS and SMM. In a result, vTZ successfully defends several kinds of attacks, such as code-reuse attacks, DMA attacks, debugging attacks and code tempering attacks.

However, vTZ also has some disadvantages. vTZ is not compatible to the existing commercial hypervisor. In vTZ, the hypervisor is not allowed to have sensitive instructions related to address translations. In addition, the module, CFLock should run in hypervisor to support vTZ. So the hypervisor must modify their source code in order to run on vTZ. That is a huge disadvantage to the promotion and application.

In conclusion, vTZ is mostly close to our goal Secure EL2 project. vTZ is also a close competitor of our project. We want

to compare the performance with vTZ and proof the advantage of our one.

### B. TEEv

TEEv is another TEE virtualization architecture to provide restricted TEEs, i.e. vTEEs. These vTEEs are concurrent in runtime and isolated from each other. (More about vTEE). A tiny hypervisor, TEE-visor, running in Secure World to manage these vTEEs and to provide isolation between vTEEs. It allows each vTEE from different manufacturers to host their own TA.

To address the challenge of the lack of TrustZone virtualization support, TEEv deploys the TEE-visor and vTEEs at the same privilege level, secure EL1. In addition, TEEv modified the commercial TEE by scanning vTEE's binary to remove the MMU-related instructions, so that TEE-visor can exclusively control the MMU. Controlling the MMU, TEE-visor can protect itself in security and confidentiality, and isolate vTEEs by protecting each vTEE's entries. As a result of removing the sensitive instruction, TEE-visor is responsible for the communication between vTEE and corresponding client application (CA). In details, TEE-visor handles the request from CAs and verify the page access from TA to CA. For isolation of vTEEs and REEs, TEE-visor manage the page table exclusively in order that each vTEE and each REE can only access their own page. Similar to vTZ, TEE-visor protect the kernel of vTEEs by setting their kernel as read only.

## IV. INTRODUCTION

This demo file is intended to serve as a “starter file” for IEEE conference papers produced under L<sup>A</sup>T<sub>E</sub>X using IEEE-tran.cls version 1.8b and later. I wish you the best of success.

mds

August 26, 2015

### A. Subsection Heading Here

Subsection text here.

1) *Subsubsection Heading Here*: Subsubsection text here.

## V. CONCLUSION

The conclusion goes here.

## ACKNOWLEDGMENT

The authors would like to thank...

## REFERENCES

- [1] H. Kopka and P. W. Daly, *A Guide to L<sup>A</sup>T<sub>E</sub>X*, 3rd ed. Harlow, England: Addison-Wesley, 1999.