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 domian in CPU who is isolated from TEE.

History of TEE.

Histroy of virtualization.

Histroy 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 hardwared-assisted base virtualization(not SEL2)

II. 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 achieve by the software. The represensative 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 shared 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 make use of the existed TEE architecture instead of design a new one. vTZ seperate the funcutionality and security by running another VM in normal world as guest TEE to serve the VM. The security is ensure by the TrustZone hardware isolation. In details, a tiny monitor in secure world control the memory mapping and world switching. A Constrained Isolated Execution Environment (CIEE) provides isolation.

The vTZ design is shown in figure. There are four secure module 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 allow 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 to 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 ensure the correction 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 execption control flow from tempering by protecting exception vector table. CFlock can 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 contiain the software implementations of TrustZone. In other words, vTZ does not utilize all the hardware in considerations 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.

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

The advantages of vTZ is 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 lines of code, which is far less than one who putting a 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 defenses 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 exisiting commercial hypervisor. In vTZ, the hypervisor is not allow to have sensitive instructions related to address translations. In addition, the module, CFLock should run in hypervisor to support vTZ. So the hypervisor must modified 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 goals Secure EL2 project. vTZ is also a close competiter of our project. We want to compare the performance with vTZ and proof the advantage of our one.

III. Introduction

This demo file is intended to serve as a "starter file" for IEEE conference papers produced under LaTeX using IEEEtran.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.

IV. Conclusion

The conclusion goes here.

Acknowledgment

The authors would like to thank...

References

[1] H. Kopka and P. W. Daly, *A Guide to LaTeX*, 3rd ed. Harlow, England: Addison-Wesley, 1999.