Panel Discussion RISC-V Day Tokyo (2019/September/30)

Position

TEE on RISC-V

National Institute of Advanced Industrial Science and Technology (AIST)

Cyber Physical Security Research Center (CPSEC)
Kuniyasu Suzaki (須崎 有康)

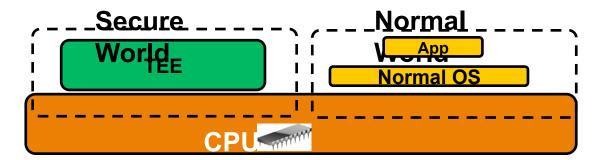


Do you know TEE?



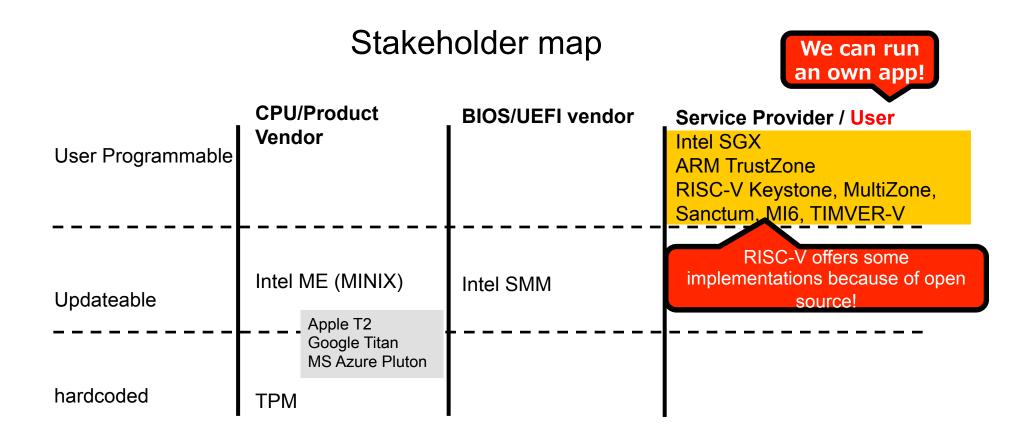
Do you know TEE?

- TEE means "Trusted Execution Environment".
- TEE offers a Hardware-assisted Isolated Execution Environment from normal Operating system.
 - Intel SGX (Software Guard eXecutions)
 - ARM TrustZone
 - RISC-V offers some implementations because of open source!
 - Keystone, MultiZone, Sanctum, MI6, TIMVER-V
 - RISC-V Foundation has TEE Working Group (AIST is a member!)





What is different from other isolated execution?





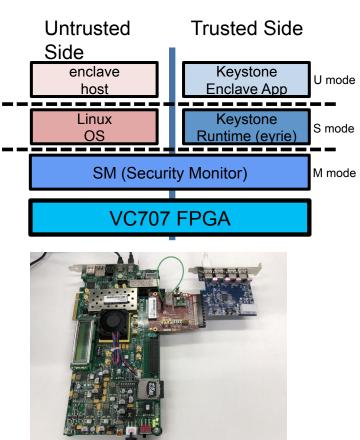
We customized Keystone on FPGA.

Verifier client

Remote Attestation

Remote PC







RISC-V TEE Research Map

RISC-V Foundation has **TEE Working Group**IETF discusses a new protocol "**TEEP (Trusted Execution Environment Provisioning)**" to manage Trusted Application in TEE (AIST works for TEEP).

UC Berkeley Keystone

Krste Asanovic https://kevstone-enclave.org/

HexFive MultiZone

Cesare Garlati
Don Barnetson
https://hex-five.com/

MIT Sanctum, MI6 Srini Devadas

llia Lebedev Victor Costan https://

www.csail.mit.edu/ research/sanctumsecure-processor

Timber-V

Graz University of Technology, Samuel Weiser TU Darmstadt, Ahmad-Reza Sadeghi

U of Minho Multizone Sandro Pinto



Key person

この成果は、国立研究開発法人新エネルギー・産業技術総合開発機構(NEDO)の委託業務「高効率・高速処理を可能とするAIチップ・次世代コンピューティングの技術開発/革新的AIエッジコンピューティング技術の開発/セキュアオープンアーキテクチャ基盤技術とそのAIエッジ応用研究開発」の結果得られたものです。

NICTA seL4 on Keystone Gernot Heiser https://sel4.systems/