

Confidential Compute for RISC-V Platforms

AP-TEE TG proposal - Ravi Sahita

Contributors - Suresh Sugumar, Andy Dellow, Manuel
Offenberg, Nick Kossifidis, Dong Du, Dingji Li, Vedvyas
Shanbhogue, Yann Loisel, Kailun Qin and others from
Trusted Computing SIG

Assignee - Security HC

Outline

Introduction to Confidential Compute

Gaps Analysis

Strategy and AP-TEE TG proposal

Charter overview and roadmap

Confidential Computing

Confidential Computing is the protection of data in use by performing computation in a Hardware-based Trusted Execution Environment.

This definition is independent of topological location, which processor does it, and whether encryption or some other isolation technique is used.

The protection of data in use is against a well-defined adversary.

Key properties of a HW-based TEE for Conf. Comp.

A Trusted Execution Environment (TEE) is an environment that provides a level of assurance of three key properties:

- Data confidentiality
- Data integrity
- Code integrity

Additional desirable characteristics:

- Code confidentiality
- Authenticated Launch
- Programmability
- Attestability -- *This is a required from the RISC-V Trusted Computing SIG perspective*
- Recoverability

Confidential Compute Threat Model

User/System Software attacks

Protocol attacks

Cryptographic attacks

Basic hardware attacks

Basic upstream supply-chain attacks

Advanced hardware attacks

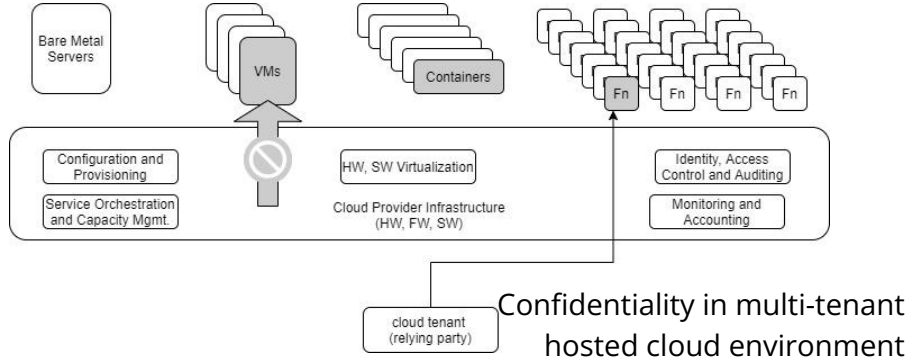
Upstream hardware supply-chain attacks

uArch and Arch Side-channel attacks*

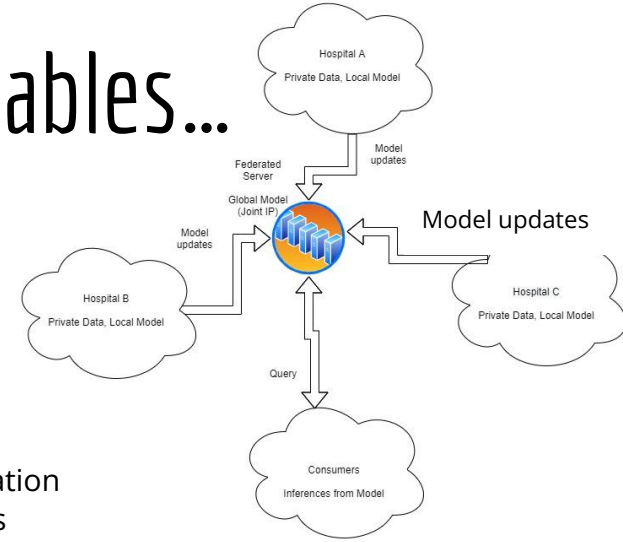
Detailed Confidential compute threat model has been defined and documented [here](#).

The RISC-V TC SIG does not aim to specify any threats from this set as out of scope - noting that different implementations will have varying degrees of resistance to these attacks.

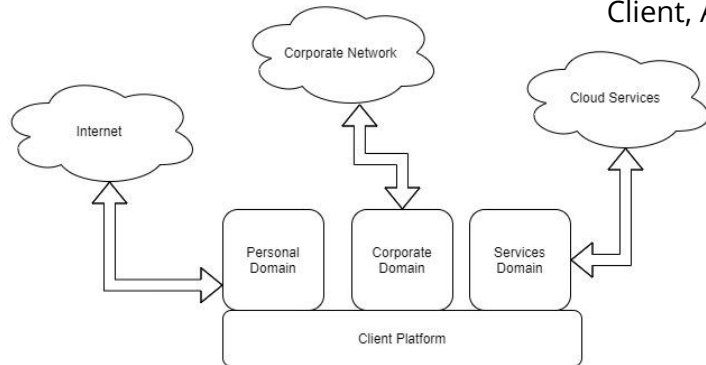
Use cases confidential compute enables...



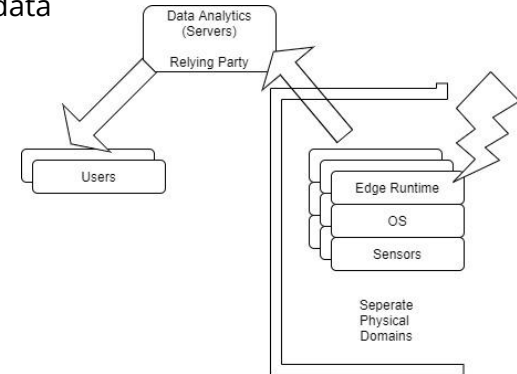
Multi-party computation on CPU/Accelerators



Multi-domain Platforms - Client, Automotive,



Edge/IOT-based data analytics



RISC-V Gaps → AP-TEE TG Charter

Why should we do this? And why now?

- Confidential Computing is at an inflection point and all compute domains/market segments (Data Center/Servers to Embedded) require support for it - alternate architectures have solutions in place => Risk to lose market share and RISC-V adopters in these domains.

Intel SGX, TDX
AMD SEV-ES-SNP
ARM Trustzone, CCA
IBM PEF
RISC-V ?

What are the gap areas? And what is our proposed action plan?

- Security Platform Model TG -- *ongoing*
- Proposed - AP-TEE TG to cover Reference Arch, Interfaces, Uncover potential ISA gaps**
 - AP-TEE Interfaces - uses current ISA; extensible to future ISA (via gap analysis) -- normative spec.
 - AP-TEE Security Arch for CC -- also use as an Implementers Guide -- informative living doc.
 - ISA proposal(s) -- request FT/TG only if needed -- normative spec.

RISC-V AP-TEE TG
addresses this gap

Who else do /should we work with?

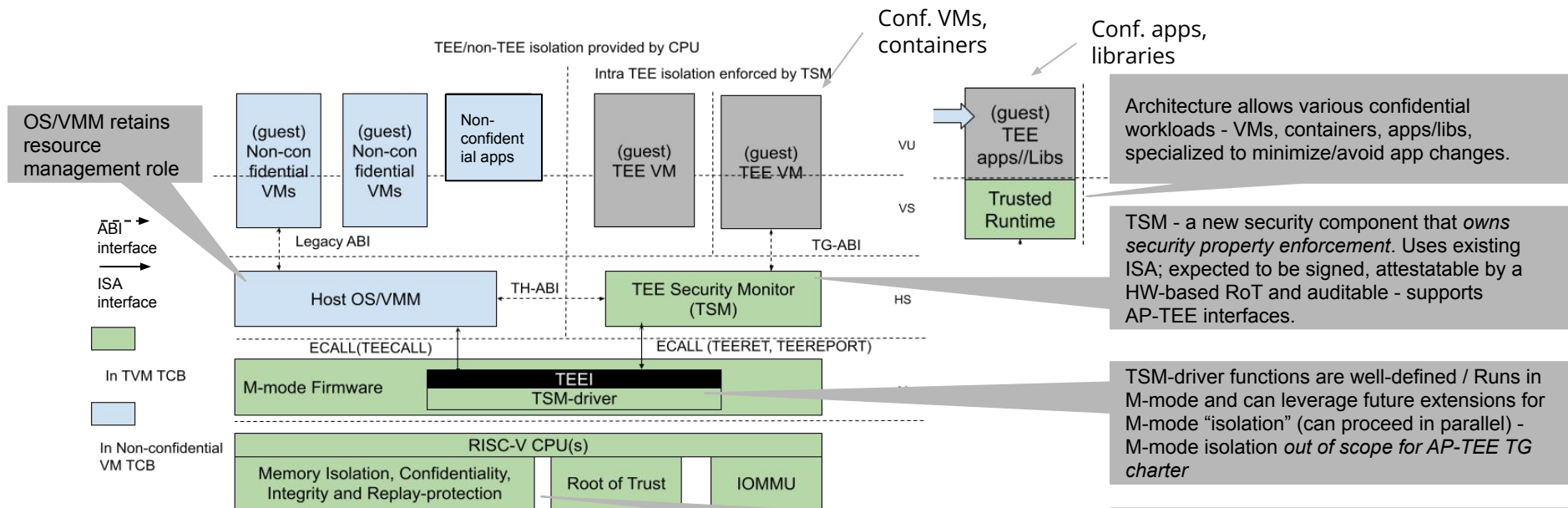
- Within RVI** - Security HC/Trusted Computing SIG, TEE TG, CFI SIG, Software HC (Hypervisor SIG), SOC infrastructure SIG (IOMMU, QoS, RAS ...), DataCenter SIG
- Outside RVI** - Confidential Computing Consortium (CCC), Trusted Computing Group (TCG), Internet Engineering Task Force (IETF), Distributed Management Task Force (DMTF), GlobalPlatform, PCIe, CXL

CCC
Open Enclave SDK
Keystone
Project Veraison

IETF RATS
TCG DICE
DMTF SPD
PCIe IDE, TDISP

AP-TEE TG Charter: Reference Arch

AP-TEE interfaces allow confidential compute models to be built using the ratified RISC-V ISA (with implementation specific micro-architecture and platform support)



For comments/feedback spec is at:

<https://docs.google.com/document/d/1TXiuy4ac3hQmEKvtTtM5aFVHLnNKCryXeRZFYPQRq2Xw/edit#>

AP-TEE TG Charter: Interface specs

Specs



POCs



Area	Function	Resources
AP-TEE TH-ABI	SBI Extension Interface implemented by the TSM via ECALL for use by OS/VMM to manage TVMs	TG WG members
AP-TEE TG-ABI	SBI Extension Interface implemented by the TSM via ECALL for use by TVM guest workloads	
TEE Security Manager (TSM)	TSM is a RISC-V 64 bit SW module that uses RISC-V H-extension and implements TH and TG-ABI. It is in the TCB for all TVM workloads (Expected to be HW-vendor signed and may be HW-operator signed)	Rivos contributes to start collab.
M-mode FW	Minimal SBI extensions (TCB component) to support TSM initialization, TEECALL, TEERET implementation. It is in the TCB for all TVM workloads (Expected to be HW-vendor signed and may be HW-operator signed) - Collab with OpenSBI	Expecting collaborators on these existing projects from Software HC
Linux, KVM (Host OS/VMM)	<i>Untrusted</i> (enlightened) host OS/VMM that manage resources for TVM-based confidential workloads [TSM enforces security properties] - Collab with Hypervisor SIG	
Linux (TVM Guest OS), Guest Firmware	Enlightened guest OS/runtime (in TCB of TVM workload) - Collab with SW HC	

AP-TEE TG Charter: Platform & ISA (Scope)

Area	Function	Resources
CPU	Evaluate AP-TEE mode qualifier, Sparse (page-based) confidential memory access-control	TG members
IOMMU	AP-TEE mode qualifier; Sparse (page-based) confidential memory access-control and fabric i/f	w/ IOMMU TG
TLB, Caches	AP-TEE mode qualifier and other micro-architectural structures	TG members
Interconnect, Fabric	Platform-specific cryptographic memory isolation and mode qualifier	TG members to document + Implementation feedback
Memory	Platform-specific cryptographic memory isolation and mode qualifier	
HW Root-of-trust	Platform-specific subsystem to support HW Attestation, Sealing interfaces	
Devices	Device-specific subsystem to support Device attestation, link security	
QoS, RAS, DC	Platform-specific, Domain-specific	w/ SOC Infra

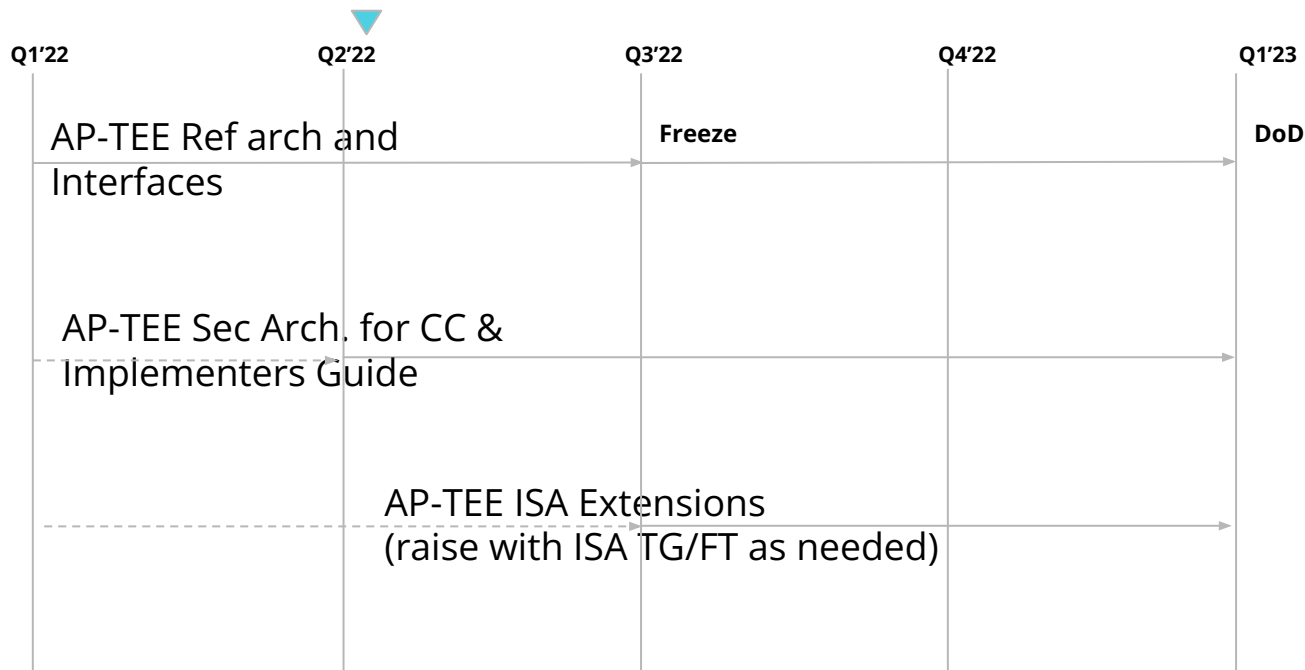
AP-TEE Security Arch for CC and Implementers Guide covers recommendations on:

- Mapping of mitigations to threat model
- Recommendations for crypto modes
- Attestation protocols, formats

Proposed AP-TEE TG workstreams

- [Proposed ratification plan](#)
- [DoD checklist](#)
- [Infra requirements](#)

-
- Initial [AP-TEE spec](#) being discussed at the TC SIG.
 - [Confidential Computing Survey](#)



Seeking Chairs, TSC Approval to form AP-TEE TG w/ this charter

(AP-TEE TG charter)

The RISC-V Application Platform - Trusted Execution Environment Task Group (AP-TEE TG) will collaborate to define the reference architecture for confidential computing on RISC-V platforms - including the ABI required to enable systems software to manage confidential workloads on a multi-tenant platform, while keeping the OS/hypervisor and entities that develop the OS/VMM and/or operate/manage the platform outside the TCB. The TG will design the interfaces to comprehend existing (ratified) ISA and ensure extensibility of the interfaces to new Architectural ISA extensions as required for security or performance of confidential workloads. In addition to the normative specifications mentioned, the TG will produce an AP-TEE-specific security architecture analysis per the confidential computing threat model agreed upon as a living (non-normative) document supporting security recommendations, implementation-specific guidelines and relevant standard protocols for attestation for implementers of the AP-TEE capability on RISC-V platforms. The proposed RISC-V AP-TEE task group will collaborate to define these three specifications:

*a. **AP-TEE reference architecture and SBI extension interface (non-ISA, normative)** which specifies the TH-ABI and TG-ABI interfaces to enable the OS/Hypervisor to manage confidential workloads on a multi-tenant platform, while keeping the OS/hypervisor and entities that develop the OS/VMM and/or operate/manage the platform outside the TCB. The interfaces are defined between:*

*1. A new platform-specific security service called the Trusted Security Manager (TSM) operating in RISC-V HS-mode and a general-purpose OS/Hypervisor executing in S/HS-mode - called the **TH-ABI**. The TH-ABI should cover aspects of: TVM creation and tear down, TVM measurement and attestation, TVM memory management and protection, TVM virtual-hart state management and protection, TVM execution and IO.*

*2. A Trusted Security Manager (TSM) running in HS-mode and a general-purpose OS executing in VS-mode - called the **TG-ABI**. The TG-ABI should cover aspects the TVM is involved in: TVM measurement extension and attestation, TVM memory conversion, TVM IO and other services used from host*

*b). **AP-TEE architecture security analysis (non-normative living document)** supporting recommendations and implementation guidelines for e.g. coverage of threat model, attestation protocols, crypto modes*

*c). **AP-TEE ISA extensions (normative)** to be proposed as needed for enforcing confidential workload security and performance requirements. The interfaces in item a. will be defined to be extensible to any such future ISA extensions. The TG will start with the definition of the programming interfaces and identify ISA gaps. ISA proposals made will be modeled via tools such as QEMU/Spike.*

*The goal of the AP-TEE interface specification is to **enable open-source reference implementations of the RISC-V AP-TEE interfaces** for platform-specific TSM implementations that enable confidential compute and trusted execution for different use case scenarios (Server, Automotive, Embedded etc.). To support this goal, a POC is defined that consists of: An SBI extension implementation for AP-TEE will be used as a reference implementation. A TSM implementation will be developed by the community as part of the ratification of the interfaces. The required changes will be made to the Linux/KVM host and guest software to validate the interface specifications.*