RISC-V TEE TG meeting

August 16, 2022

RISC-V TEE Architecture

Goals, Assumptions, Approach, Plans

Guerney D H Hunt
IBM T.J. Watson Research Center
presenter

Wojciech Ozga
IBM Research - Zurich

Outline

- Goals
- Assumptions
- Evolution
- Threat models
- Requirements

Goals

- Describe an incremental approach to build trusted execution environment (TEE) for RISC-V.
  - Support different threat/performance/complexity use cases:
    - Low-high-tier embedded
    - Edge
    - High performance computing (HPC) / cloud
- Clarify which features are needed for the full set of RISC-V use cases.

Assumptions

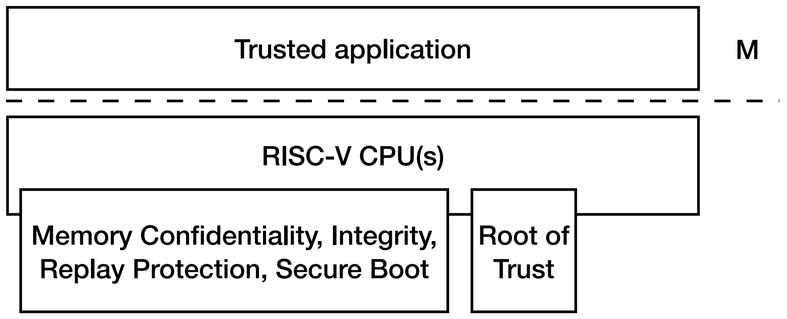
We assume the presence of certain functionalities:

- Secure and trusted boot (trusted computing SIG),
- IOMMU (IOMMU TG),
- Memory system support (Run Time integrity SIG(?)),
    - Memory controller, paging architecture.

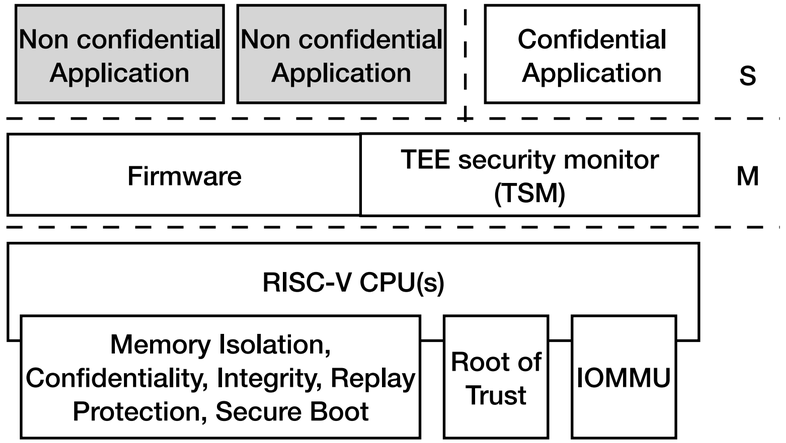
Evolution

- Embedded devices -> Edge -> HPC/Cloud.
- Proposed iterative approach:
  - Start with the minimal approach (minimal/no architectural changes).
  - What are the limitations of this approach?
  - What can be done to provide more security guarantees, increase performance, scalability?
  - Propose required changes for more complex TEE models.

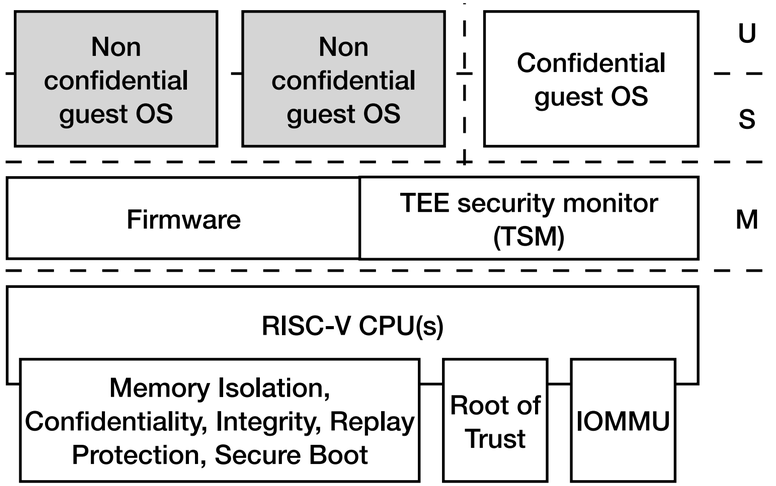
Embedded Deployment Models



Model 1: Single application deployment (low-end embedded).

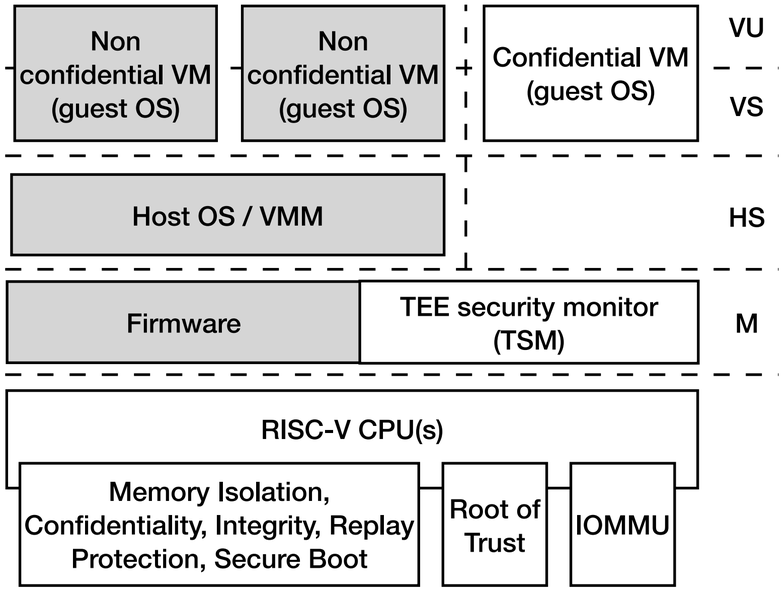


Model 2: Multi-application deployment (mid-tier embedded).

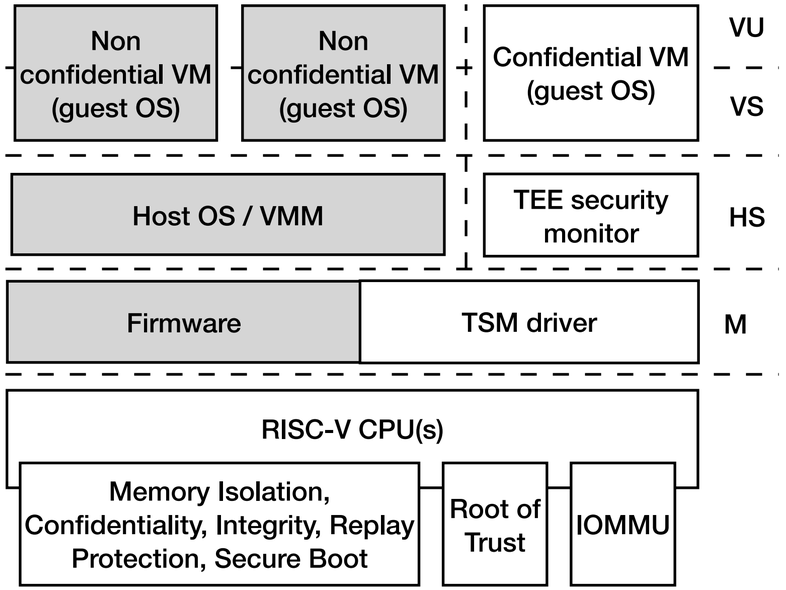


Model 3: Multi-OS deployment (high-end embedded).

Modified Deployment Model

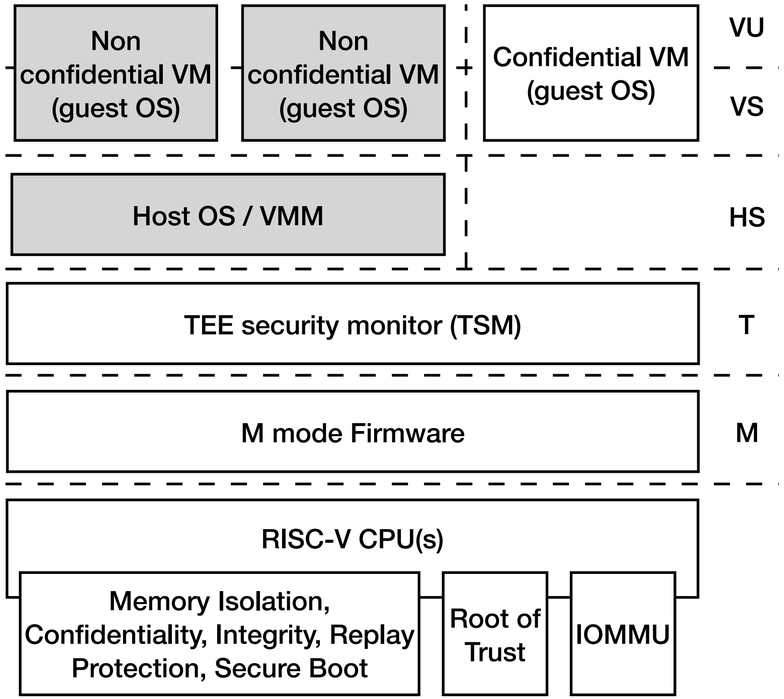


Model 4: M-mode split.

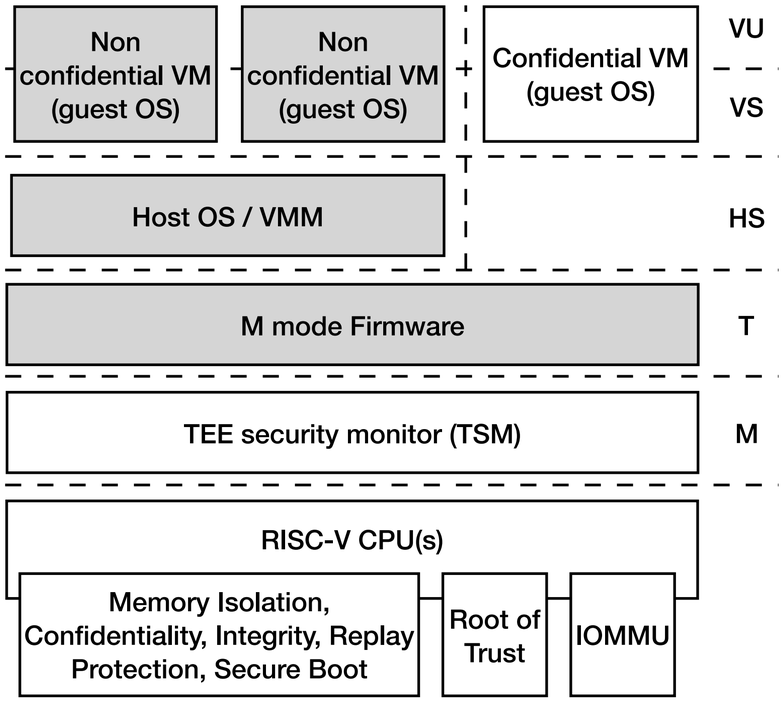


Model 4 (current): M-mode and HS-mode split.

Additional Deployment Models



Model 5: New stage.



Model 6: Untrusted firmware.

Threat Models

Deployment models operate under different threat models. For example:

Example threat models

	Cloud/HPC	**Edge**	**High-end embedded**	**Low-end embedded**
Security domains (shared resources)	Multiple tenants	Multiple/Single tenant	Single tenant	Single tenant
Local software-level attacker	Untrusted hypervisor	Untrusted hypervisor/OS	Untrusted applications/ OS	None
Remote software-level attacker	Yes	Yes	Yes	No (air gapped devices)
Hardware attacker (physical attacks)	No (defense in depth at the data centre level)	Yes/No	Yes	Yes
Malicious DMA devices	Yes/No	Yes/No	Yes	Yes/No

Requirements

- On the next slide we present the security requirements defined by the community.
- We added additional deployment models and introduced changes.
- We use the following colour notation:

No changes compared to the original requirements defined by the community	A definition or meaning changed.	Security criteria accepted by the community	Security criteria that is out of scope for the given deployment model

- Assign required security criteria to each deployment model: Isolation, Accessibility, Addressability, Integrity, Confidentiality, Freshness.

Category	Security Criteria	Cloud / HPC	Edge	High-end Embedded	Low-end Embedded	Required if	Examples	RVI HC/SIG/TG
Memory Footprint	Stolen/reserved memory	Minimize					Recording meta data of secure memory	AP-TEE TG specify
TEE CPU State Protection	State Isolation	Required	Required	Required	Out of scope		Prevent untrusted code from arbitrarily accessing/modifying TEE CPU state	AP-TEE TG specify
Memory Confidentiality	Memory isolation	Required	Required	Required	Out of scope		Prevent untrusted components from reading TEE memory	AP-TEE TG specify
	Cipher text read prevention	Optional	Optional	Out of scope	Out of scope		Prevent untrusted code from accessing encrypted TEE memory	AP-TEE TG specify
	Per TEE encryption	Optional	Optional	Out of scope	Out of scope	Multiple security domains	Each VM has one or more unique keys	AP-TEE to recommend
	Memory encryption strength	Optional	Optional	Optional	Optional		Encryption algorithm and key strength	AP-TEE to recommend
	Number of encryption keys	Optional	Optional	Out of scope	Out of scope		Number of TEE keys supported	AP-TEE to recommend
Memory Integrity	Memory integrity against SW attacks	Required	Optional	Optional	Out of scope	Multiple security domains	Prevent SW attacks such as remapping, aliasing, replay, corruption, etc.	AP-TEE TG specify
	Memory integrity against HW attacks	Optional	Required	Optional	Optional		Prevent HW attacks, DRAM-bus attacks and physical attacks that replace TEE memory with old data	AP-TEE to recommend
	Memory execution isolation	Required	Optional	Required	Out of scope	Multiple security domains	Prevent TEE from executing from normal memory	AP-TEE TG specify
	Rowhammer attack prevention	Optional	Optional	Optional	Out of scope		Prevent untrusted code from flipping bits of TEE memory	AP-TEE to recommend
Shared Memory	TEE controls data shared with untrusted code	Required	Optional	Optional	Out of scope	Multiple security domains	Prevent malicious code from exfiltrating information without TEE consent/opt-in	AP-TEE TG specify
	TEE controls data shared with another TEE	Required	Optional	Optional	Out of scope	Multiple security domains	Ability to securely share memory with another TEE	AP-TEE TG specify
Memory Assignment	Ability to make memory secure/normal	Required	Optional	Optional	Out of scope	Multiple security domains	Secure memory should be dynamically allocated/unallocated as required	AP-TEE to specify, priviledge architecture
I/O Protection	DMA protection from untrusted devices	Required	Required	Optional	Optional	DMA	Prevent untrusted peripheral devices from accessing TEE memory	AP-TEE TG specify
	Trusted I/O from trusted devices	Optional	Optional	Optional	Optional	Untrusted devices	Bind devices to TEEs	IOMMU,APTTT to specify
Secure IRQ	Trusted Interrupts	Required	Required	Required	Required		Prevent IRQ injections that violate priority or masking	AIA, AP-TEE to specify
Secure Timetamp	Trusted timestamps	Required	Required	Required	Required		Ensure TEE have consistent timestamp view	AP-TEE TG specify
Debug Profile	Trusted performance monitoring unit	Required	Optional	Optional	Out of scope		Ensure TEEs get correct PMU info; prevent data leakage due to PMU information (fingerprint attacks)	Performance SIG
	Debug support	Required	Optional	Optional	Out of scope		Support debug registers	Debug TG
	Authenticated debug (Production device)	Required	Optional	Optional	Out of scope		Ensure hardware debug prob (e.g., JTAG, SWD) is disabled in production	AP-TEE TG specify
Availability	Untrusted TEE DoS Protection	Required	Optional	Optional	Out of scope	Multiple security domains	Prevent untrusted TEE from refusing to exit	AP-TEE TG specify
	Untrusted code DoS Protection	Out of scope	Out of scope	Out of scope	Out of scope		Prevent untrusted code from refusing to run TEE	N/A ?
Side Channel	Protected address mapping (controlled side channel)	Required	Optional	Optional	Out of scope	Multiple security domains	Similar to memory remapping attacks	uSG SIG, AP-TEE specify
	u-architectural side channels (branch prediction,..)	Required	Optional	Optional	Out of scope	Multiple security domains	Prevent attacks such as meltdown/spectre (it is difficult to defend agains such attacks in advance)	uSG SIG, AP-TEE specify
	Control channels, single-step/zero-step defence	Required	Optional	Optional	Out of scope	Multiple security domains	Prevent interrupt/exception injection (combined with cache side channel to leak sensitive data)	uSG SIG, AP-TEE specify
	Architectural cache side channel	Optional	Optional	Optional	Out of scope	Multiple security domains	e.g. prime probe	uSG SIG, AP-TEE specify
	Architectural timing side channel	Optional	Optional	Optional	Out of scope	Multiple security domains	Leveraging data dependency timing channels	uSG SIG, AP-TEE specify
Secure and measured boot	Establishes root of trust in support of attestation	Required	Required	Required	Required		Knowing that initial firmware is authorised and correct version , …	Security Model TG
Attestability	Remote attestation	Required	Required	Optional	Out of scope	Internet	Prevent fake hardware and software TCB; Prevent malicious hardware debugging in production.	AP-TEE TG specify
	Mutual attestation	Optional	Optional	Optional	Out of scope	S/U mode	Attestation to another TEE on the same platform	AP-TEE TG specify
	Remote mutual attestation	Required	Optional	Optional	Out of scope	Internet	Attestation to a TEE on a different platform	AP-TEE TG specify
	Local attestation	Required	Optional	Required	Required	Sealing	Verification of attestation by TCB	AP-TEE TG specify
	TCB versioning	Required	Required	Optional	Optional	Mutable firmware	Prevent TCB rollback	AP-TEE TG specify
	TCB transparency (and auditability)	Optional	Optional	Optional	Optional	Mutable firmware	TCB elements reviewable	AP-TEE TG recommend
Operational Features	Sealing	Required	Required	Optional	Optional		Binding of secrets to TEEs	AP-TEE TG specify
	Migration	Required	Optional	Out of scope	Out of scope		Secure migration of TEEs	Hypervisor SIG, AP-TEE TG specify
	Nesting	Required	Out of scope	Out of scope	Out of scope		Nested TEE Workloads	Hypervisor SIG, AP-TEE TG specify

Current approach

Agreements:

- Current approach would meet the needs of cloud scenarios.
  - Recommend simplification
  - AP-TEE will have to work with other groups in RISC-V.
- Remote attestation is needed.
  - Recommend additional forms.
- Hardware ROT and secure and measured boot.
- Small as possible TSM
  - Provable TSM.
- Need (in some models) for an updatable TSM.
- Need (for cloud/HPC) to change the classification of pages. Pages can be trusted, untrusted or in transition. An API has been proposed
- We agree that DOS protection is out of scope.

Questions:

- Focuses only on the cloud scenario which comes with increased complexity.
  - Designing without the perspective of the other use case may introduce unnecessary incompatibilities.
- Top-bottom approach does not guarantee TEEs for other use cases.
- Can we reduce the number of context switches?
  TSM in a HS-mode AP-TEE-mode (TSM driver + TSM). Too many context switches between trusted und untrusted world.
- API complexity. Can we convert the VM into TEE in one call?
- We do not understand the definition of the memory footprint requirement.

Backup slides

TEE Secure Monitor (TSM)

- Challenges:
  - Provable secure and certifiable
  - Minimize the codebase size - minimal set of features inside of the TCB
  - Upstream Linux kernel support
- We can start with the **open source** version [1] of the TSM used for OpenPOWER [2]
  - ~75k LoC
  - Supported by Linux kernel, QEMU/KVM

[1]: https://github.com/open-power/ultravisor
[2]: Hunt et al., Confidential computing for OpenPOWER. In Proceedings of the Sixteenth European Conference on Computer Systems (EuroSys '21), 2021.

Category	Security Criteria	Requirements for RVI	Example	RVI HC/SIG/TG
Memory Footprint	Stolen/Reserved memory	Avoid/Minimize	*Recording metadata of secure memory*	*AP-TEE TG specify*
CPU State Protection	State Isolation	Required	*Prevent untrusted VMM from arbitrarily accessing/modifying vCPU state*	*AP-TEE TG specify*
Memory Confidentiality	Memory isolation (confidentiality)	Required	*Prevent untrusted components from reading plaintext VM memory*	*AP-TEE TG specify*
	Memory encryption strength	Implementation-specific	*Encryption algorithm & key length*	*AP-TEE TG Recommend*
	Per VM encryption	Implementation-specific	*Each VM has a unique key*	*AP-TEE TG Recommend*
	Number of encryption keys	Implementation-specific	*Number of VM keys supported*	*AP-TEE TG Recommend*
Memory Integrity	Memory isolation (integrity)	Required	*Prevent untrusted VMM from modifying VM memory*	*AP-TEE TG specify*
	Ciphertext access prevention	Required	*Prevent untrusted VMM from accessing encrypted VM memory*	*AP-TEE TG specify*
	Rowhammer attack prevention	Implementation-specific	*Prevent untrusted VMM from fliping memory bits of VMs; https://arxiv.org/pdf/2201.02986.pdf*	*AP-TEE TG Recommend*
	Memory integrity against SW attacks	Required	*Prevent SW attacks such as replay, corruption, remapping, aliasing, etc.*	*AP-TEE TG specify*
	Memory integrity against HW attacks	Implementation-specific	*Prevent HW attacks such as DRAM-bus attacks*	*AP-TEE TG Recommend*
	SW Replay protection	Required	*Prevent untrusted VMM from replacing VM memory with old data*	*AP-TEE TG specify*
	HW Replay protection	Implementation-specific	*Prevent physical attacks that replace VM memory from old data*	*AP-TEE TG Recommend*
Shared Memory	Workload control over data shared with untrusted host	Required	*Prevent malicious host from exfiltrating information without VM consent/opt-in*	*AP-TEE specify*
I/O Protection	DMA protection from untrusted devices (basic)	Required	*Prevent peripheral devices from accessing VM memory*	*AP-TEE specify*
	Trusted IO from trusted devices	Implementation-specific	*Bind devices to TVMs*	*IOMMU TG, AP-TEE specify*
Secure IRQ	Trusted Interrupts	Required	*Prevent vIRQ injections that violate priority or masking*	*AIA TG, AP-TEE TG specify*
Secure Timestamp	Trusted Timestamps	Required	*Ensure VMs have consistent timestamp view*	*AP-TEE TG specify*
Debug & Profile	Trusted Performance Monitor Unit (PMU)	Required	*Ensure VMs get correct PMU info; Prevent data leakage due to PMU info (fingerprint attacks)*	*Perfmon SIG*
	Debug support	Required	*Support debug registers*	*Debug TG*
	Authenticated debug (production/dev)	Required	*Ensure hardware debug probe (e.g., JTAG, SWD) is disabled in production*	*AP-TEE specify*
Availability	CVM --> VMM DOS protection	Required	*Prevent untrusted VMs from refusing to exit*	*AP-TEE specify*
	VMM --> CVM DOS protection	Out of Scope	*Prevent untrusted VMM from refusing to run VMs*	*NA*
Side-channel	Protected Address Mapping (also a controlled side channel)	Required	*Similar to memory remapping attacks*	*uSC SIG, AP-TEE specify*
	uArch side channels (branch predictor poisoning, etc.)	Required*	*Prevent attacks such as meltdown/spectre (it is difficult to defend against such attacks in advance)*	*uSC SIG, AP-TEE specify*
	Controlled-channels a.k.a single step/zero-step defense	Required	*Prevent malicious interrupt/exception injection (combined with cache side channel to leak sensitive data)*	*uSC SIG, AP-TEE specify*
	Architectural Cache Side channel	Implementation-specific	*e.g. prime / probe*	*uSC SIG, AP-TEE specify*
	Architectural Timing Side channel	Implementation-specific	*leveraging data dependency timing channels*	*uSC SIG, AP-TEE specify*
Attestability	Remote Attestation [related but unique from Secure boot]	Required	*Prevent faked hardware and software TCB; Prevent malicious hardware debugging in production.*	*AP-TEE TG specify*
	Local Attestation	Implementation-specific	*Attestation to another TVM on the same platform*	*AP-TEE TG specify*
	TCB versioning	Required	*Prevent TCB rollback*	*AP-TEE TG specify*
	TCB transparency (and auditability)	Desirable, Impl-specific	*TCB elements reviewable*	*AP-TEE TG Recommend*
	Sealing	Required	*Binding of secrets to confidential VMs*	*TC SIG, Secure Boot TG*
Operational features	Migration	Required	*Migration of confidential workloads*	*Hypervisor SIG, AP-TEE specify*
	Nesting	Required	*Nested TVM workloads*	*Hypervisor SIG, AP-TEE specify*
	QoS, RAS interop	Implementation-specific	*Interop with QoS, RAS features for TVM workload*	*QoS SIG specify*

Current Deployment Models